NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
116-390 Village Boulevard
Princeton, New Jersey 08540-5721
Phone: 609.452.8060 ▪ Fax: 609.452.9550
www.nerc.com

NAESB
North American Energy Standards Board
1301 Fannin, Suite 2350
Houston, Texas 77002
Phone: 713.356.0060 – Fax 713.356.0067
www.naesb.org

Joint Interchange Scheduling Working Group Meeting
Development of E-Tag 1.8

Thursday, November 15, 2007, 1 p.m.–5 p.m. PDT
Friday, November 16, 2007, 9 a.m.–Noon, PDT

Doubletree Hotel San Francisco Airport
835 Airport Blvd.
San Francisco, CA
Hotel Phone: (650) 344-5500

Conference Bridge (Call-in):
Phone Number: (732) 694-2061
Thursday Access Code: 1123111507#
Friday Access Code: 1123111607#

Participation via WebEx webcast
Location: https://nerc.webex.com/nerc
Topic: E-Tag
Thursday Password: 111507
Friday Password: 111607

Agenda

1. Administrative

a. Membership and Guests — Chair
b. Arrangements — Secretary
c. Approval of Meeting and Conference Call Minutes:
   i) August 29, 2007, JISWG Meeting Minutes — Chair
   ii) October 3, 2007, JISWG Meeting Minutes — Chair
d. Procedures
   i) Parliamentary Procedures — Secretary
   ii) Antitrust Compliance Guidelines — Secretary
e. Approval of Agenda

2. e-Tag 1.8 — Chair

a. e-Tag 1.8 Project Implementation Plan
b. Vendor Information Sharing Techniques
c. Recap of the e-Tag 1.8 Interoperability Vendor Testing
d. e-Tag 1.8 Cutover Plan
e. Tuesdays BA-to-BA-to-Vendor Interoperability Testing
f. Terminology Within e-Tag 1.8

3. TSIN Registry transition from NERC to NAESB — Chair

4. Future JISWG Meetings/conference calls

JISWG Meeting	December 19–20, 2007	Houston
JISWG Meeting	January 23–24, 2008	West Palm Beach, FL
JISWG Meeting	March 19–20, 2008	Houston
JISWG Meeting	May 21–22, 2008	San Diego
JISWG Meeting	July 23–24, 2008	Halifax
JISWG Meeting	September 24–25, 2008	Eureka, CA or Colorado Springs, CO
JISWG Meeting	November 12–13, 2008	Houston

Item 1.a Membership and Guests

Co-chairs Jim Hansen and Bob Harshbarger will welcome the Joint Interchange Scheduling Working Group (JISWG) members, e-Tag vendors, and guests. The chairs will ask members and guests to introduce themselves.

Attachment

Attendance list to be provided at the meeting

Item 1.b Arrangements

The JISWG Meeting will begin on Thursday, November 15 at 1 p.m. and adjourn by noon on Friday, November 16. Lunch will be provided to the meeting attendees on Thursday.

Item 1.c Approval of Meeting and Conference Call Minutes

The chair will ask for review and approval of the draft JISWG Meeting and conference call minutes.

- August 29, 2007, JISWG Meeting Minutes
- October 3, 2007, JISWG Meeting Minutes

Attachment

1. August 29, 2007, JISWG Meeting Minutes — Chair
2. October 3, 2007, JISWG Meeting Minutes — Chair

Item 1.d Procedures

Item 1.d.i. Parliamentary Procedures

A summary of Parliamentary Procedures is attached for reference. The chair and secretary will answer questions regarding these procedures.

Item 1.d.ii. Antitrust Compliance Guidelines

On June 14, 2002, the NERC Board of Trustees adopted Antitrust Compliance Guidelines for NERC. In adopting the guidelines, the board passed the following resolution:

RESOLVED, that the Board of Trustees (1) adopts the draft Antitrust Compliance Guidelines attached hereto as Exhibit A and (2) instructs that these Antitrust Compliance Guidelines be included in the agenda package for each meeting of every NERC committee, subcommittee, task force, working group, and other NERC-sponsored activity.

The resolution also applies to workshops, training sessions, and any other NERC-sponsored event. A copy of the NERC Antitrust Compliance Guidelines will be included in the agenda package for each meeting of each group or event.

Attachments

1. Parliamentary Procedures
2. Antitrust Compliance Guidelines

Item 1.e Approval of Agenda

The chair will ask for approval of the Interchange Subcommittee (IS) meeting agenda.

Item 2. E-Tag 1.8 — Chair

The electronic interchange tagging system e-Tag 1.8, implementation will take place on December 4, 2007. The JISWG will perform a final review of all aspects of the implementation plan and cutover plan to ensure there are no obstacles or show stoppers to the current plans.

In addition to the IS review, the JISWG asked the IS to consider any e-Tag 1.8 implementation show stoppers. If the IS does not present a legitimate reason to delay or stop the e-Tag 1.8 implementation plan, the JISWG is prepared to go forward as scheduled with the implementation plan.

The JISWG also needs a response from the vendors whether they completed all the structured testing the JISWG developed.

Discussion

The JISWG will discuss the following items and determine if the e-Tag 1.8 scheduled implementation plan will go forward.

Item 2.a e-Tag 1.8 Project Implementation Plan

Jim Hansen and Bob Harshbarger will lead the JISWG discussion of the e-Tag specifications, schema, comment form, and implementation plan. The JISWG and e-Tag Vendors have devoted a lot of time and energy to develop the documents in preparation for implementation of e-Tag 1.8 on December 4, 2007. The JISWG and e-Tag Vendors are asked to review the implementation plan and bring any discrepancy, correction, or recommendation to the attention of the JISWG.

E-Tag 1.8 Project Implementation Plan			
Tentative Completion Dates	Purpose	Location	Status
March 19, 2007	Develop e-Tag 1.8 project plan Training Industry conference calls • Two in Eastern Interconnection • Two in Western Interconnection Interoperability testing	Conference call	c
March 20, 2007	IS approve e-Tag 1.8 project plan by e-mail ballot between 3/19/2007–3/23/2007 by 12:00 a.m. ET	E-mail ballot, tallied by Don Lacen	c
March 23, 2007	Develop list of questions for comment and overview or "what's new" document		c
March 23, 2007	Contingent on IS approval — Post e-tag specification 1.8, e-Tag 1.8 schema, project plan, and "what's new" document, questions, for 30-day industry comment period (March 23–April 23, 2007)	Post on NERC and NAESB websites, comments to be returned to JISWG list server (details to be worked out)	c
May 2,3 2007	IS/JISWG Joint Meeting — Portland, OR		c
May 3, 2007	Post response to industry comments (IS and JISWG responses and incorporate changes to the final plan)	Post on NERC and NAESB websites (details to be worked out)	c
May 15–16, 2007	JISWG Meeting	Houston, TX	c
July 12, 2007	JISWG Meeting 9 a.m.–5 p.m.	San Diego, CA	c

July 13, 2007	JISWG to develop structured interoperability test starting June 13, 2007	1 month development	c
July 30–31, 2007	JISWG Meeting 10 a.m.–5 p.m., 9 a.m.–2 p.m.	Houston, TX	c
August 1, 2007	JISWG, NERC, and NAESB meeting — registry long term solution	Houston, TX	c
August 5, 2007	Vendor development (May 3–August 5, 2007)		c
August 7, 2007	ESS/ITS conference call — Finalize conditional firm design changes for e-Tag		c
August 6–24, 2007	Interoperability vendor testing • NERC/NAESB (JISWG) Facilitation • 8/7, 8/9, 8/13, 8/15, 8/20, and 8/22	Vendors conduct remotely	c
August 29–30, 2007	JISWG Meeting 9 a.m.–5 p.m., 9 am.–noon — finalize tutorial	Vancouver, BC, Canada	c
September 4, 6, and every Tuesday thereafter	Vendors will make their e-Tag approval and authority service (as applicable) available for unstructured interoperability testing. Approval services should be set to automatically actively approve all requests.	8 a.m.–5 p.m. central time	
September 14, 2007	Redlined revised e-Tag 1.8 specification for conditional firm		c
September 19–20, 2007	IS Meeting	Montreal, Canada	c
September 7, 11, and 25, 2007	Industry tutorial/Q&A/Information sharing (September)	Three conference calls/webcasts — Two hours each	c
September 21, 2007	JISWG/IS review of revised specification completed, release to vendors for implementation		c
Oct 3–4, 2007	JISWG 10 a.m.–5 p.m.,9 a.m.–2 p.m.	Houston, TX	c
October 22, 2007	Vendor development for conditional firm	Pending above	c
October 22, 2007	Vendor unstructured testing, specifically for conditional firm but other testing allowed as needed		c
October 29, 2007	Vendor unstructured testing, specifically for conditional firm but other testing allowed as needed		
November 2, 2007	User training and testing — Industry participants and vendors may use the time between September 7–November 2, 2007 to train their users and modify their back office software as necessary to incorporate 1.8 changes (September 7–November 2, 2007)	As determined by vendors and participants	
Nov 5–9, 2007	Interoperability Testing — final		
November 14–15, 2007	IS Meeting	San Francisco, CA	
November 15–16	JISWG Meeting 1–5 p.m., 9 a.m.–noon	San Francisco, CA	
December 4, 2007	**E-Tag 1.8 — Implementation**		

December 19–20	JISWG 10 a.m.–5 p.m., 9 a.m.–noon	Houston, TX	

Item 2.b Vendor Information Sharing Techniques

Informing the commercial power industry of the changes from the current e-Tag 1.7.097 to the new e-Tag 1.8 is a challenge for the JISWG and the e-Tag vendors. The JISWG and e-Tag vendors have spent considerable time developing a strategy to accomplish this task by prepared informational webcasts, presenting industry tutorials, Q&A, information sharing techniques, posting NERC and NAESB meeting announcements and supporting documentation, and industry vendor testing.

The e-Tag 1.8 vendors, will coordinate future instructions with their clients and Balancing Authorities (BAs) to ensure they understand and implement e-Tag 1.8 on December 4, 2007. The e-Tag 1.8 schema, specifications, conditional firm specifications, tutorial, and Q&A are attached for reference.

Attachment

1. e-Tag 1.8 Schema (sent under seperate cover)
2. e-Tag 1.8 Specifications
3. e-Tag 1.8 Conditional Firm Specifications
4. e-Tag 1.8 Frequently Asked Questions (Q&A)
5. e-Tag 1.8 Tutorial — PowerPoint Presentation

Item 2.c Recap of the e-Tag 1.8 Interoperability Vendor Testing

Brett Fisher coordinated and facilitated the e-Tag 1.8, interoperability vendor testing that took place on August 7, 9, 13, 15, 2007. Mr. Fisher reported the vendor tests were performed successfully.

Any additional testing that the JISWG, e-Tag vendors, or NERC — NAESB wholesale electric quadrant thinks is necessary, needs to voice their recommendations so that the BA-to-BA-to-vendor interoperability testing can be performed. See agenda item 2.3, below.

Item 2.d e-Tag 1.8 Cutover Plan

The JISWG modified the cutover plan to decrease the time for 1.7 e-tags; to resolve and increase time for 1.7 to 1.8 conversion; and to remove the requirement to terminate e-tags that do not contain at least one BA in SE field.

The cutover plan is attached for the JISWG and e-Tag vendors to perform a final review.

Attachment

e-Tag 1.8 Cutover Plan

Item 2.e Tuesday BA-to-BA-to-Vendor Interoperability Testing

A couple of vendors have requested that we schedule and monitor additional structured interoperability vendor testing. In order for us to lower risk associated with e-Tag 1.8 implementation, the JISWG Chairs recommend the JISWG pick a date (preferably a Tuesday) and a test monitor (or maybe a tag team of test monitors) to coordinate and facilitate the testing. OATI has requested that any structured testing be conducted after November 7, 2007.

JISWG Chair Hansen believes the vendors should start the test in reverse order to try to ensure that they hit all the tests prior to the December 4, 2007 “go live date” and that they should use SSL on the server side at least.

Item 2.f Terminology Within e-Tag 1.8

The JISWG and e-Tag vendors need to review all documents to ensure the terminology is properly defined, referenced, and understood. Issues or concerns on the terminology need to be brought forth to the JISWG as soon as possible to resolve and document appropriately.

The JISWG and e-Tag vendors have spent a tremendous amount of time preparing to implement e-Tag 1.8. Any misunderstanding that anyone has in regards to the e-Tag 1.8 implementation need to be resolved to ensure communications are clear, unambiguous, and consistent.

Please identify any misunderstood or confusing terminology or language that needs additional enhancement for the purposes of thorough understanding to the JISWG during this meeting.

Item 3. TSIN Registry Transition from NERC to NAESB — Chair

The Transmission System Information Network (TSIN) Registry transition from the North American Electric Reliability Corporation (NERC) to the North American Energy Standards Board (NAESB) is anticipated to be complete in 2008. NAESB has requested the JISWG review and discuss the TS I N Registry Rewrite, System Requirements Document for technical accuracy. The last version of the document was generated on August 22, 2006 and may need enhancements to meet the current technical requirements.

Action
The JISWG will discuss, begin to review, and to update/enhance the TSIN Registry Rewrite System Requirements Document for technical accuracy. Additional JISWG face-to-face meetings or webcasts will be scheduled as necessary to meet the NAESB schedule.

Attachments:

1. TSIN Registry Rewrite System Requirements Document
2. TSIN Registry Rewrite Request for Information

Item 4. Future Meetings

Additional meetings or conference calls may be scheduled as necessary for the implementation of the e-Tag 1.8, electronic tagging registry, or other JISWG business.

JISWG 2007 Meeting/Conference Call/Webcast Schedule			
2007 JISWG Meeting Schedule			Host
Dec 19–20, 2007	19, 10 a.m.–5 p.m. 20, 9 a.m.–noon	Houston, TX	NAESB
2008 JISWG Meeting Schedule			
Jan 23–24, 2008	23, 10 a.m.–5 p.m. 24, 9 a.m.–noon	West Palm Beach, FL	NERC
Mar 19–20, 2008	19, 10 a.m.–5 p.m. 20, 9 a.m.–2 p.m.	Houston, TX Office	NAESB
May 21–22, 2008	21, 10 a.m.–5 p.m. 22, 9 a.m.–noon	San Diego, CA	NERC
Jul 23–24, 2008	23, 10 a.m.–5 p.m. 24, 9 a.m.–noon	Halifax, Nova Scotia	NERC
Sep 24–25, 2008	24, 10 a.m.–5 p.m. 25, 9 a.m.–noon	1st Choice: Eureka, CA Alt Choice: Colorado Springs, CO	NERC
Nov 12–13, 2008	12, 10 a.m.–5 p.m. 13, 9 a.m.–noon	Houston, TX	NAESB

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
116-390 Village Boulevard
Princeton, New Jersey 08540-5721
Phone: 609.452.8060 ▪ Fax: 609.452.9550
www.nerc.com

NAESB
North American Energy Standards Board
1301 Fannin, Suite 2350
Houston, Texas 77002
Phone: 713.356.0060 – Fax 713.356.0067
www.naesb.org

Joint Interchange Scheduling Working Group Meeting

August 29–30, 2007

Vancouver, BC, Canada

Meeting Minutes

A meeting of the North American Electric Reliability Corporation (NERC) and the North American Energy Standards Board (NAESB) Joint Interchange Scheduling Working Group (JISWG) was held on August 29–30, 2007 in Vancouver, BC, Canada. The meeting announcement, agenda, and attendance list are attached as **Exhibits A**, **B**, and **C**, respectively. Individual statements and minority opinions are affixed as **Exhibits D** and **E**. There were none.

JISWG co-chairs Jim Hansen and Bob Harshbarger presided.

Antitrust Compliance Guidelines

Secretary Vandervort acknowledged the NERC Antitrust Compliance Guidelines.

Minutes of the Previous Meetings

Andy Tritch moved to approve the July 6, 2007 JISWG conference call minutes. The JISWG adopted the minutes by unanimous consent.

Brett Fisher moved to approve the July 30–August 1, 2007 JISWG meeting minutes. The JISWG adopted the minutes by unanimous consent.

JISWG Roster

The JISWG discussed the option of having an official roster. NAESB generally allows anyone that participates in a meeting or conference call to have a voice and voting privileges. By unanimous consent, the JISWG will not have an official roster. However, anyone that wishes to participate in a JISWG conference call or meeting is welcome to do so. In addition, anyone that wishes to be placed on the JISWG mailing list is welcome. The "JISWG" and "JISWG_plus" list servers will be combined into a single list server ("JISWG_plus" list server will be retired). JISWG NERC Secretary Vandervort will send a note to all current "JISWG," "JISWG_plus," "tagven," and "tagging" list server members to update the contact information and to validate the e-mail lists for accuracy (anyone that does not respond to the request will be deleted from the listservers).

JISWG Members Requested to Serve on NERC Interchange Standard Drafting Team

NERC Standards Process Manager contacted the JISWG co-chair Bob Harshbarger to inquire if the group had the diversity to be considered for a NERC standard drafting team (SDT). JISWG discussed the possibility of its participating members to form the nucleus of the NERC Interchange standard drafting team to address the revised timing tables SAR. Secretary Vandervort will send a request to the JISWG list servers to determine interest in participation in the above standard drafting team.

E-Tag 1.8

JISWG co-chairs Jim Hansen and Bob Harshbarger led the JISWG and e-Tag 1.8 vendors discussion of the e-Tag specifications, schema, project implementation plan, industry tutorial/Q&A/information sharing techniques, interoperability vendor testing, and conditional firm discussion.

E-Tag 1.8 Specifications and Schema

The JISWG reviewed a number of issues within the e-Tag 1.8 specifications and the schema. A few additional modifications were made to the e-Tag 1.8 specifications to meet compliance with a revision to the NAESB Coordinate Interchange Standard and to provide correction distribution to parties who may be impacted by corrections to the energy or transmission product code. The latter is necessary for FERC Order 890 implementation. This specification will be the starting point for conditional firm modifications which will be completed by September 14, 2007.

The issues and resulting actions included the following:

- The e-Tag 1.8 specification does not address a Purchasing Selling Entity (PSE) Agent creation request submitted that does not have a start/stop on a minute boundary. Does the JISWG add the clarification to the specification?
    - The Vendors agreed to add validation that will reject any tag submitted that does not start or stop on a minute boundary.
    - The JISWG will modify the specification
- JISWG addressed the token name length identified in INT-BPS-014 (i.e. WECC_Reserve_Responsible_Entity_Type (36 characters)
  The token field is too short, currently the field is set to 32 characters. Does the JISWG increase the number of characters?
    - Expand to 128 characters in the schema
- MCG wants the JISWIG to clarify how to correctly calculate request start/end time. Should we have validation on the authority for the following?
  Request start time = earliest of energy start, transmission start, and loss accounting start
  Request end time = latest of energy stop, transmission stop, and loss accounting stop
  MCG requested that request start/end time calculations be changed to the following:
  Start time = energy start
  End time = energy stop
    - Yes, the JISWG will add a validation to require energy profile match loss accounting and transmission profile start and end.
- JISWG addressed and clarified:
  Clarify in Specification — Validation on losses — against Point of Receipt (POR) or Point of Delivery (POD) or not at all

Does a validation need to be added to the specification for validating that the Losses or transmission allocation profiles do not exceed the energy profile?

- The JISWG will modify the specification to validate that the energy profile can be accommodated by the minimum of the POR or POD transmission allocation profiles.

- JISWG will address the need to capture WECC Reserve Sharing Group (RSG) entities
  - The JISWG will develop and provide a file that contains a list of RSG members who are not balancing authorities (BA) and need to be identified as the entity responsible for contingency reserves and the file format will be CSV file, containing the Tagging Entity ID and Tag Code.
  - All of these entities would be PSEs.
  - WECC will place this file on their web site and JISWG will provide the URL to vendors.
  - When JISWG began asking for specific entities who are PSEs and responsible for the reserves, WECC reserve sharing group members began discussion whether or not such a list was required since the BAs who are actually carrying the reserves are already allocating the reserve quantities to the PSE members. RSG memebers will get back to JISWG with the list.
- Reliability limits and exceptions language within e-Tag 1.8 specification 6.1.4.2.2.2, states the reliability limit are defined for the reliability coordinators, source balancing authority, and sink balancing authority.
  The Transmission Service Providers and Scheduling Entities (those intermediate reliability entities) need to be included.
  - The JISWG will include the transmission service providers and scheduling entities (those intermediate reliability entities) into e-Tag 1.8 Specification 6.1.4.2.2.2.

The JISWG is still receptive to consider any proposed change or enhancement that the NERC and NAESB community, the e-Tag users, the e-Tag vendors, or the electric power industry recommends or proposes. Adopted suggestions or changes may be postponed for future versions of e-Tag since 1.8 changes are being kept to a minimum in order to achieve the December 5, 2007 implementation target.

E-Tag 1.8 Project Implementation Plan

The JISWG modified the e-Tag 1.8 project implementation plan to include additional testing dates, webcast dates, and to update actual dates. See **Exhibit G**.

Industry Tutorial / Q&A / Information Sharing Techniques

The JISWG will provide an overview of the changes that are incorporated into the e-Tag 1.8 specifications and schema, including the reasons for the changes, the general functionality of the e-Tag 1.8 system, and the logic behind the project process. It is the responsibility of the JISWG to describe and justify the e-Tag 1.8 system. The vendors will have the bulk of the educational system for e-Tag 1.8. The vendors will only present the changes and create the training for the new e-Tag 1.8 system (relying on the JISWG to justify the changes).

During previous JISWG meetings, it was emphasized that anyone developing e-Tag software must provide a user guide and educational programs for the use of their software in accordance with the e-Tag 1.8 specifications.

JISWG co-chair Bob Harshbarger will lead the tutorials with support from co-chair Jim Hansen, e-Tag 1.8 vendors, and other JISWG members. The JISWG encourages NERC, NAESB, and interested industry participants to participate in one of the tutorials. The tutorial webcasts details are as follows:

e-Tag 1.8 Tutorial / Questions and Answers Session / Information Sharing			
Date	***Time***	***Webcast (visual display)***	***Dial-In Audio***
September 7, 2007	2–4 p.m. CDT	Call the NAESB Office (713–356–0060). At that time, the NAESB Office will provide the URL, access code, and security code.	Phone #: 866–740–1260 Access code: 3560060 Call the NAESB Office, (713–356–0060) for a four digit security access code
September 11, 2007	2–4 p.m. CDT	Location: https://nerc.webex.com/nerc Topic: Tutorial Password: 091107	NERC Conference bridge/dial in: Phone #: 732–694–2061 Access code: 1123091107#
September 25, 2007	2–4 p.m. CDT	Location: https://nerc.webex.com/nerc Topic: Tutorial Password: 092507	NERC Conference bridge/dial in: Phone #: 732–694–2061 Access code: 1123092507#

e-Tag 1.8 Interoperability Vendor Testing

Brett Fisher coordinated and facilitated the e-Tag 1.8, interoperability vendor testing that took place on August 7, 9, 13, and 15. Mr. Fisher and the e-Tag 1.8 vendors reported on the vendor testing that took place and summarized the conclusions and recommendations.

Mr. Fisher thanked all vendors that participated in the testing. He thought the test went very well. Some e-Tag 1.8 vendors were not able to participate in the test. If the JISWG has specific parameters that need to be addressed or evaluated, then all vendors including those that were not able to participate in the vendor interoperability testing, should consider testing their software.

Starting on Tuesday, September 4, 2007 and continuing on every Tuesday, from 8 a.m. to 4 p.m., central prevailing time, the e-Tag 1.8 vendors will make their authority and approval service available to perform vendor interoperability testing. Balancing authorities, transmission service providers, and load serving entities are encouraged to contact their vendors to test any parameters they desire. Vendors will be able to interface with other vendors by planning and scheduling the desired testing during the Tuesday windows.

Conditional Firm

The JISWG discussed what was necessary to incorporate the FERC Order 890 "Conditional Firm" parameters into e-Tag 1.8. The JISWG drafted the preliminary specification for implementation of conditional firm in e-Tagging document, **Attachment F**. Messers. Hansen and Harshbarger will incorporate the conditional firm specifications into the e-Tag 1.8 specifications by September 14 and then allow a one week comment period for industry review and input to the revised specifications. Vendor development and testing will proceed with milestones on October 22 and 29. The e-Tag 1.8 — conditional firm schedule is as follows:

Date (2007)	***Responsibility***	***Action***
Sep 14	JISWG	Incorporate conditional firm specs into e-Tag 1.8 specifications
Sep 17–21	NERC/NAESB/Industry	Comment window for e-Tag 1.8 specifications with conditional firm criteria
Oct 22	e-Tag 1.8 Vendors	Vendor development of conditional firm formatting
Oct 29	e-Tag 1.8 Vendors	Operational structured vendor testing of e-Tag 1.8 conditional firm criteria
Oct 29–Nov 29	JISWG	Enhance e-Tag 1.8 after vendor conditional firm testing is complete

NAESB Request R07007

The NAESB Executive Committee remanded R07007 back to the JISWG to consider the comments of Ed Davis of Entergy and to hold the business practice standard until the corresponding NERC reliability SAR process is complete. The JISWG reviewed the NAESB Executive Committee draft meeting minutes and the comments submitted by Ed Davis (after the comment period had ended) on behalf of Entergy, see the JISWG August 29–30 meeting agenda.

The comments raised concerns regarding the creation of new rows in the timing table that JISWG had introduced in order to re-introduce the time classifications of "on time" and "late" and to specify the new "ATF" time classification in the standards. Mr. Davis stated that the addition of the new row associated with "late" would require additional, compliance sanctionable, active response requirements. Mr. Davis commented that current standards do not require active response for e-Tags that are late.

The JISWG and participants on the phone discussed the comments and reviewed the existing standards. While some of those present agreed that active approval or denial should not be required for e-Tags that would be classified as "late." The standards state that active response is required and the consensus of the JISWG meeting was that current standards required active response for any e-Tag that may be submitted, including those that would be classified as "late" and "after the fact." Therefore R07007 does not create additional, compliance sanctionable, approval requirements. Any entity or individual may submit a standards authorization request (SAR) to modify current standards.

The JISWG will, as stated in the EC motion, wait until the NERC SAR process is final to take further action with R07007. Note that the NERC SAR process is underway, see the "JISWG Members Requested to Serve on NERC Interchange Standard Drafting Team," located in these meeting minutes.

Transaction Default Ramp Duration

Larry Goins has questioned the JISWG's selection of zero as a default ramp duration for reliability adjustments and would like the default to be changed to ten minutes for the Eastern Interconnection and 20 minutes for the Western Interconnection consistent with the NAESB coordinate interchange standards. The JISWG members do not have a vested interest in what the default ramp duration is as long as it can be modified to non-default values by the approval. The JISWG considered the following:

- The current INT Standards do not contain ramp duration specifications or requirements.
- The NAESB Coordinate Interchange Standards do not apply to reliability adjustments, and are instead specific to hourly scheduling intervals ("spread evenly over the top of the hour").
- The current default ramp rate used in e-Tagging is zero.
- According to OATI, the Interchange Distribution Calculator (IDC) needs to see a zero ramp rate.
- Many BA's assume zero to mean "as soon as possible" and ramp at whatever rate their physical system allows.
- The approval services can very easily be set up to default a different ramp rate. This exists in most systems already.
- Physical ramp rate will vary by system and over time based on units on-line, etc. This impacts ramp duration.
- For a curtailment call where system reliability is impacted, "as soon as possible" is usually what the reliability entity desires.
- For adjustments that impact future hours, the operator has more time to change the default ramp duration.

In light of this discussion, the JISWG determined that the default ramp duration for reliability adjustments will remain as specified in e-Tag 1.8 until such time as INT Standards are modified to specify a different duration. The e-Tag specification is not a standard; therefore, reliability entities may implement whatever duration they feel is appropriate (since no standards apply to ramp duration). Any entity wishing a different default duration may wish to contact the vendor of their approval software to ensure that a different default may be specified.

e-Tag Registry

The JISWG created and submitted a NAESB Project Plan R06007, Develop a Wholesale Registry for the Wholesale Electric Quadrant. The project will designate NAESB as the entity that is responsible for contracting with a vendor on behalf of industry participants to provide, update, and maintain a revised registry.

JISWG NERC Secretary Vandervort will contact the appropriate NERC staff to ensure the NERC Technical Committee agrees with this plan. With NERC and NAESB authorization, the JISWG will initiate action on the R06007 registry project.

Dates and Locations of Future Meetings

Additional meetings or conference calls may be scheduled as necessary for the implementation of the e-Tag 1.8.

JISWG 2007 Meeting/Conf Call/Webcast Schedule				
	Date	*Time*	*Location*	*Coordination*
e-Tag 1.8 Tutorial Webcast	Fri, Sep 7	2–4 pm, CDT	Webcast	NAESB
e-Tag 1.8 Tutorial Webcast	Tues, Sep 11	2–4 pm, CDT	Webcast	NERC
e-Tag 1.8 Tutorial Webcast	Tues, Sep 25	2–4 pm, CDT	Webcast	NERC
Meeting	Wed, Oct 3 Thur, Oct 4	10 am–5 pm 9 am–2 pm	Houston, TX	NAESB
Meeting	Thur, Nov 15 Fri, Nov 16	1 pm–5 pm 9 am–Noon	San Francisco, CA	NERC (Follows the IS Meeting)
Meeting	Wed, Dec 19 Thur, Dec 20	10 am–5 pm 9 am–Noon	Houston, TX	NAESB

Respectfully submitted,

Tom Vandervort

Thomas J. Vandervort
Joint Interchange Scheduling Working Group NERC Secretary

Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 10th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and can not reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	Yes	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." Otherwise, this motion is debatable and subject to 2/3 majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The "seconder" is not recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary,, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.

Notes on Voting

(Recommendations from DMB, not necessarily Mr. Robert)

Abstentions. When a member abstains, he is not voting on the Motion, and his abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

Determining the results. The results of the vote (other than Unanimous Consent) are determined by dividing the votes in favor by the total votes cast. Abstentions are not counted in the vote and shall not be assumed to be on either side.

"Unanimous Approval." Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

Majorities. Robert's Rules use a simple majority (one more than half) as the default for most motions. NERC uses 2/3 majority for all motions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC ANTITRUST COMPLIANCE GUIDELINES

I. GENERAL

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. PROHIBITED ACTIVITIES

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

Approved by NERC Board of Trustees, June 14, 2002
Technical revisions, May 13, 2005

116-390 Village Boulevard, Princeton, New Jersey 08540-5721
Phone: 609.452.8060 ▪ Fax: 609.452.9550 ▪ www.nerc.com

III. ACTIVITIES THAT ARE PERMITTED

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.

- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.

- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Electronic Tagging
Functional Specification

Version 1.8.0

APPROVED FOR IMPLEMENTATION

September 20, 2007

Joint Interchange Scheduling Work Group

North American Electric Reliability Corporation

Table of Contents

SECTION 1 - FUNCTIONAL DESCRIPTION 8

1.1 INTRODUCTION 8
1.1.1 PURPOSE 8
1.1.2 E-TAG REFERENCES 8
1.1.3 CHANGE LOG 8
1.2 DEFINITIONS 10
1.3 TAGGING TERMINOLOGY 18
1.4 SYSTEM CONCEPTS 21
1.4.1 SYSTEM ARCHITECTURE 22
1.4.1.1 Agent Service 22
1.4.1.2 Authority Service 22
1.4.1.3 Approval Service 23
1.4.1.4 Reliability Authority Service 23
1.4.2 TAG IDENTIFICATION 23
1.4.2.1 E-Tag IDs 23
1.4.2.2 Security Keys 24
1.4.3 TEST E-TAGS 25
1.4.4 COMMUNICATIONS 25
1.4.4.1 Method Types 25
1.4.4.1.1 Requests 25
1.4.4.1.2 Request Distributions 26
1.4.4.1.3 Actions 26
1.4.4.1.4 Information Distributions 26
1.4.4.1.5 Queries 26
1.4.4.1.6 Callbacks 26
1.4.4.2 Message Size Limitations 26
1.4.5 FINANCIAL AND PHYSICAL PATHS 26
1.4.6 PROFILE DESCRIPTIONS 27
1.4.7 TRANSMISSION ALLOCATION 31
1.4.8 TIMING REQUIREMENTS 32
1.4.8.1 Approval of Reliability Changes 32
1.4.9 TAG AUDITING 33
1.4.9.1 Message Rejection Log 33
1.4.9.2 Historical e-Tag Archive 33
1.4.9.3 Statistics 33
1.4.9.4 Authority Off-Line Archive 33
1.4.10 ROUNDING 34
1.4.11 CARBON COPY LIST 34
1.5 TRAINING REQUIREMENTS 35
1.5.1 USER GUIDES 35
1.5.2 USER EDUCATION 35
1.6 FUNCTIONAL CONCEPTS 36
1.6.1 INITIATING A REQUEST 36
1.6.1.1 Submitting a New e-Tag Request 36
1.6.1.2 Submitting a Correction Request 36
1.6.1.3 Submitting a Profile Change Request 37
1.6.2 REQUEST DISTRIBUTION 37
1.6.2.1 Distributing a New e-Tag Request 37
1.6.2.2 Distributing a Correction Request 37
1.6.2.3 Distributing a Profile Change Request 38

1.6.3 E-TAG REQUEST ACTIONS 38
1.6.3.1 Approving and Denying Requests 38
1.6.3.2 Withdrawing a Request 39
1.6.3.3 Canceling a Request 39
1.6.3.4 Terminating an e-Tag 39
1.6.4 INFORMATION DISTRIBUTION 40
1.6.4.1 Distribution of Request Approval State 40
1.6.4.2 Distribution of Request Resolution 40
1.6.4.3 Distribution of Potential TLR Profile Change 40
1.6.5 QUERY FUNCTIONS 40
1.6.5.1 Querying for e-Tag Summaries 41
1.6.5.2 Querying for an e-Tag 41
1.6.5.3 Querying for e-Tags 41
1.6.5.4 Querying for an e-Tag's History 42
1.6.5.5 Querying for Request IDs 42
1.6.5.6 Querying for a Specific Request 42
1.6.5.7 Querying for a Specific Request's State 42
1.6.5.8 Querying for Service Availability 42

SECTION 2 - TAG AGENT FUNCTIONAL REQUIREMENTS 43

2.1 INTRODUCTION 43
2.2 REGISTRY USAGE 44
2.3 TAG DATA ENTRY AND VIEWING 44
2.3.1 TAG ID CREATION 44
2.3.2 SECURITY KEY CREATION 44
2.4 DATE AND TIME HANDLING 44
2.5 DATA VALIDATION 45
2.6 FUNCTION IMPLEMENTATION 45
2.6.1 INITIATING A REQUEST 45
2.6.1.1 Submitting a New e-Tag Request 46
2.6.1.2 Submitting a Correction Request 46
2.6.1.3 Submitting a Profile Change Request 47
2.6.2 REQUEST DISTRIBUTION 48
2.6.2.1 Processing a New e-Tag Request Distribution 48
2.6.2.2 Processing a Correction Request Distribution 49
2.6.2.3 Processing a Profile Change Request Distribution 49
2.6.3 REQUEST ACTIONS 49
2.6.3.1 Approving and Denying Requests 49
2.6.3.2 Withdrawing a Request 49
2.6.3.3 Cancelling an e-Tag 50
2.6.3.4 Terminating an e-Tag 50
2.6.4 INFORMATION DISTRIBUTION 51
2.6.4.1 Processing a Request Approval State Distribution 51
2.6.4.2 Processing a Request Resolution Distribution 51
2.6.4.3 Processing a Potential TLR Profile Change Distribution 52
2.6.5 QUERY FUNCTIONS 52
2.6.5.1 Synchronous Queries 52
2.6.5.1.1 Query for an e-Tag 53
2.6.5.1.2 Query for Request IDs 53
2.6.5.1.3 Query for a Request 53
2.6.5.1.4 Query for a Request's State 53
2.6.5.1.5 Querying for System Availability 53
2.6.5.2 Asynchronous Queries 53
2.6.5.2.1 Query Summaries 54

2.6.5.2.2 Query e-Tags 55
2.6.5.2.3 Query History 55
2.7 AVAILABILITY AND PERFORMANCE 55

SECTION 3 - TAG AUTHORITY FUNCTIONAL REQUIREMENTS 56

3.1 INTRODUCTION 56
3.2 REGISTRY USAGE 56
3.3 TAG DATA ENTRY AND VIEWING 57
3.3.1 APPROVAL STATE OVERRIDE 57
3.3.2 SECURITY KEYS 57
3.4 DATE AND TIME HANDLING 57
3.5 DATA VALIDATION 58
3.6 FUNCTION IMPLEMENTATION 59
3.6.1 INITIATING A REQUEST 59
3.6.1.1 Processing a New e-Tag Request Submission 59
3.6.1.1.1 Identifying the Distribution List 60
3.6.1.2 Processing a Correction Request Submission 62
3.6.1.3 Processing a Profile Change Request Submission 62
3.6.2 REQUEST DISTRIBUTION 66
3.6.2.1 Distributing a New e-Tag Request 67
3.6.2.2 Distributing a Correction Request 67
3.6.2.3 Distributing a Profile Change Request 68
3.6.3 REQUEST ACTIONS 68
3.6.3.1 Processing Request Approvals and Denials 68
3.6.3.2 Processing a Withdraw Request 69
3.6.3.3 Processing a Terminate Request 69
3.6.4 INFORMATION DISTRIBUTION 70
3.6.4.1 Distribution of Request Approval State 70
3.6.4.2 Distribution of Request Resolution 71
3.6.4.3 Potential TLR Profile Change Distributions 71
3.6.5 RECOVERY FUNCTIONS 72
3.6.5.1 Processing Synchronous Queries 72
3.6.5.1.1 Processing an e-Tag Query 72
3.6.5.1.2 Processing a Request Ids Query 72
3.6.5.1.3 Processing a Request Query 72
3.6.5.1.4 Processing a Request State Query 73
3.6.5.1.5 Processing Queries for System Availability 73
3.6.5.2 Processing Asynchronous Queries 73
3.6.5.2.1 Processing e-Tag Summary Queries 74
3.6.5.2.2 Processing an e-Tags Query 74
3.6.5.2.3 Processing an e-Tag History Query 75
3.7 AVAILABILITY AND PERFORMANCE 75

SECTION 4 - TAG APPROVAL FUNCTIONAL REQUIREMENTS 76

4.1 INTRODUCTION 76
4.2 REGISTRY USAGE 76
4.3 TAG DATA ENTRY AND VIEWING 77
4.4 DATE AND TIME HANDLING 77
4.5 DATA VALIDATION 77
4.6 FUNCTION IMPLEMENTATION 77
4.6.1 INITIATING A REQUEST 78
4.6.1.1 Submitting a Correction Request 78

4.6.1.2 Submitting a Profile Change Request 79
4.6.2 REQUEST DISTRIBUTION 80
4.6.2.1 Processing a New e-Tag Request Distribution 81
4.6.2.2 Processing a Correction Request Distribution 81
4.6.2.3 Processing a Profile Change Request Distribution 81
4.6.3 REQUEST ACTIONS 81
4.6.3.1 Approving and Denying Request 82
4.6.3.2 Withdrawing a Request 82
4.6.4 APPROVAL SERVICE INFORMATION DISTRIBUTION 83
4.6.4.1 Processing a Request Approval State Distribution 83
4.6.4.2 Processing a Request Resolution Distribution 83
4.6.4.3 Potential TLR Profile Change Distributions 83
4.6.5 RECOVERY FUNCTIONS 83
4.6.5.1 Synchronous Queries 83
4.6.5.1.1 Query for an e-Tag 84
4.6.5.1.2 Query for Request Ids 84
4.6.5.1.3 Query for a Request 84
4.6.5.1.4 Query for a Request's State 84
4.6.5.1.5 Query for System Availability 84
4.6.5.1.6 Processing Queries for System Availability 84
4.6.5.2 Asynchronous Queries 84
4.6.5.2.1 Query Summaries 85
4.6.5.2.2 Query e-Tags 86
4.6.5.2.3 Query History 86
4.7 AVAILABILITY AND PERFORMANCE 87

SECTION 5 - RELIABILITY AUTHORITY SERVICE 88

5.1 INTRODUCTION 88
5.2 REGISTRY USAGE 88
5.3 E-TAG DATA ENTRY AND VIEWING 88
5.4 DATE AND TIME HANDLING 88
5.5 DATA VALIDATION 88
5.6 FUNCTION IMPLEMENTATION 88
5.6.1 INITIATING A REQUEST 89
5.6.1.1 Submitting a Profile Change Request 89
5.6.2 REQUEST DISTRIBUTION 89
5.6.2.1 Processing a New e-Tag Request Distribution 90
5.6.2.2 Processing a Correction Request Distribution 90
5.6.2.3 Processing a Profile Change Request Distribution 90
5.6.3 INFORMATION DISTRIBUTION 90
5.6.3.1 Processing of a Request Resolution Distribution 90
5.6.3.2 Distribution of a Potential TLR Profile Change 90
5.7 AVAILABILITY AND PERFORMANCE 91

SECTION 6 - DATA MODEL OVERVIEW 92

6.1 TAG DATA 92
6.1.1 TRANSACTION TYPES 92
6.1.2 MARKET SEGMENTS 92
6.1.2.1 Scheduling Responsibilities 93
6.1.2.2 Title Transfers 93
6.1.3 PHYSICAL SEGMENTS 93
6.1.3.1 Generation 94

6.1.3.2 Transmission 94
6.1.3.2.1 Scheduling Entities 94
6.1.3.3 Load 95
6.1.4 PROFILE SETS 95
6.1.4.1 Profile Types 96
6.1.4.1.1 Market Level 96
6.1.4.1.2 Reliability Limit 96
6.1.4.1.3 Dynamic Minimum Energy 96
6.1.4.1.4 Dynamic Maximum Energy 96
6.1.4.1.5 Current Level 96
6.1.4.2 Profile Usage 96
6.1.4.2.1 Base Profiles 97
6.1.4.2.2 Exception Profiles 97
6.1.4.2.2.1 Market Level Exceptions 97
6.1.4.2.2.2 Reliability Limit Exceptions 97
6.1.5 TRANSMISSION ALLOCATIONS 98
6.1.5.1 Base Allocation Profiles 98
6.1.5.2 Exception Allocation Profiles 98
6.1.6 LOSS ACCOUNTING 98

SECTION 7 - MESSAGING OVERVIEW 99

7.1 MESSAGING CONCEPTS 99
7.1.1 USE OF THE TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL 99
7.1.1.1 Establishing Connections 100
7.1.1.1.1 Partial Connection Failures 100
7.1.1.1.2 Combining Messages 101
7.1.2 USE THE HYPERTEXT TRANSPORT PROTOCOL 101
7.1.2.1 HTTP/S Requests 101
7.1.2.2 HTTP/S Responses 101
7.1.3 HOW SMXP WORKS 102
7.1.4 METHOD TYPES 103
7.1.4.1 Requests 103
7.1.4.2 Request Distributions 103
7.1.4.3 Actions 103
7.1.4.4 Information Distributions 103
7.1.4.5 Queries 103
7.1.4.6 Callbacks 104
7.1.5 FAULTS 104
7.1.6 RETURN VALUES 104
7.1.7 ERROR MESSAGES 104
7.2 METHOD DESCRIPTIONS 104
7.2.1 SPECIAL DATA STRUCTURES 105
7.2.1.1 Tag ID 105
7.2.1.2 Message Info 105
7.2.1.3 Return State 105
7.2.1.4 Miscellaneous Info 105
7.2.2 ERRORS AND ERROR LISTS 106
7.2.3 INITIATING A REQUEST 107
7.2.3.1 Special Data Structures 107
7.2.3.1.1 TimeClassification 107
7.2.3.2 Request New Tag 107
7.2.3.3 Request Correction 107
7.2.3.4 Request Profile Change 108
7.2.4 REQUEST DISTRIBUTION 108

7.2.4.1 Special Data Structures 108
7.2.4.1.1 Approval Rights Flag 108
7.2.4.1.2 Impact Flag 109
7.2.4.2 Distribute New e-Tag 109
7.2.4.3 Distribute Correction 109
7.2.4.4 Distribute Profile Change 109
7.2.5 REQUEST ACTIONS 110
7.2.5.1 Set State 110
7.2.5.2 Withdraw Request 111
7.2.5.3 Terminate Request 111
7.2.6 INFORMATION DISTRIBUTION 112
7.2.6.1 Distribute Status 112
7.2.6.2 Distribute Resolution 112
7.2.6.3 Distribute Potential TLR Profile Change 112
7.2.6.4 Callback Potential TLR Profile Change 113
7.2.7 QUERY FUNCTIONS 113
7.2.7.1 Query Summaries 113
7.2.7.2 Callback Summaries 113
7.2.7.3 Query e-Tag 114
7.2.7.4 Query e-Tags 114
7.2.7.5 Callback e-Tags 114
7.2.7.6 Query History 115
7.2.7.7 Callback History 115
7.2.7.8 Query Request 115
7.2.7.9 Query Request IDs 116
7.2.7.10 Query Status 116
7.2.7.11 QueryAvailability 116

Section 1 - Functional Description

1.1 Introduction

1.1.1 Purpose

This document describes the functional requirements and detailed technical specifications for the implementation of an electronic Transaction Information System (TIS), also referred to as Electronic Tagging or just e-Tag. These requirements and specifications provide a basis for tools designed to facilitate identification and communication of interchange transaction information (e-Tags) between parties in accordance with NERC Reliability Standards and NAESB Business Practice Standards.

1.1.2 E-Tag References

Data related to the JISWG and this work can be found at
http://www.naesb.org/weq/weq_jiswg.asp

The most recent copy of the e-Tag 1.8 XML Schema can be found at
http://reg.tsin.com/Tagging/ e-Tag/

For detailed information regarding NAESB Standards, please see
http://www.naesb.org/

For detailed information regarding NERC Standards, please see
https://standards.nerc.net/

The Hypertext Transport Protocol version 1.1 is described by W3C RFC 2616 and can be obtained at
http://www.w3.org/Protocols/HTTP/1.1/rfc2616.txt.gz

The XML Schema Protocol is defined by the W3C and can be downloaded from
http://www.w3.org/2000/10/XMLSchema

The Simple Method exchange Protocol (SMXP) is defined by the OASIS Standards Collaborative and can be found on the TISWG site:
http://reg.tsin.com/Tagging/ e-Tag/

1.1.3 Change Log

Version	Change	spare
1.7096	Accepted all changes in 1.7095 posted document	

	Replaced NERC policy references with NERC/NAESB Standards references	
	Incorporated Functional Model language	
	Added Change Log	
	Updated other references and URLs	
	Market Re-dispatch (MRD) language and function removed	
1.7.097	Removed Passive Approval by Reliability Entities	
	Extend e-Tag creation to 48 hours into the past	
	Extend e-Tag adjustment to 96 hours into the past for DYNAMIC e-Tags	
	Remove 24 hour limit on Reliability Adjustments	
	Remove Counter Party Reports	
	Remove references to MRD	
	Add Optional Approval Rights for any PSE cited in the transmission allocation	
	Replaced various state diagrams with descriptive wording	
	Strike automatic approval of cancellations	
1.8	Remove Background section	
	Add reference to default ramp rate definitions	
	Add new final states and their definitions	
	Add Rounding definition	
	Add Ramp Duration validation	
	Identify physical segment in Curtailment (for proper MWh accounting when in-kind losses are used)	
	Modify in-kind loss calculations	
	Define which Functional Model entities can be Scheduling Entities (BA)	
	Strike Appendix A	
	Strike erroneous current level warning	
	Carbon Copy list (no approval, sent copies of e-Tag)	
	Calculation of ActOnByTime and ImplementTime	
	Addition of TimeClassification (Late, OnTime, ATF)	
	NERC web site changed to Electric Industry Registry web site	
	Added RequestTerminateTag and related handling	
	Simplify Recovery function	
	Allow ATF e-Tags to be Terminated	
	Allow Source or Sink to modify DYNAMIC e-Tag with actual data	
	Transmission Allocation must be $\geq$ energy profile.	
	Validations in INT-007-1 R1.1, 1.2, and 1.3 are performed by the Agent and Authority	
	Added SSL via HTTPS and client certificate requirement based on NAESB PKI standard	
	Extend e-Tag creation to 168 hours into the past	

	Extend e-Tag adjustment to 168 hours into the past for DYNAMIC e-Tags	
	Current Level no longer distributed (calculated based on approved requests in request order)	
	Change Tag Agent, Tag Approval, Tag Authority to Agent, Approval, Authority	
	Change Tag to e-Tag	
	Add Pseudo Tie tag type.	
	Add functionality to allow TSP to modify their associated physical segment's Transmission Product Reference and Transmission Allocation(s) with no approval process for support of Order 890 Conditional Firm	
	Transmission and Energy profiles must have same earliest start and latest end. Loss Accounting Profile must be bounded by (be within) these.	

1.2 Definitions

Term	Definition
{Source BA, Sink BA, PSE} Code	Entity Code defined in the Electric Industry Registry
ACTIVE	An Approval State Type indicating that a party has specifically indicated their willingness or unwillingness to implement a particular Request.
Active Approval	An approval or denial that occurred through an entity's deliberate indication of their intent.
Approval Entity	Entities identified on the transaction path of an e-Tag that have been authorized with approval rights by NERC/NAESB standards.
Approval Rights	The rights that an entity has to approve, deny, curtail, or otherwise modify an e-Tag.
Approval State	The State communicating an Approval Entity's willingness to implement a particular Request.
Approval State Type	A description of the manner in which an Approval Entity's State was set.
APPROVED	Approval State indicating that an entity is willing to implement a Request. This is also the Request State and is achieved when either all entities with approval rights on the Request have submitted their approvals, or the market assessment period has expired and all reliability entities (BA, TSP, SE) have approved the Request and no market entities (GPE, LSE, or PSE whose transmission rights are cited) have denied the Request. Once a Request reaches this state, an e-Tag is created or modified as called for by the Request.

Arranged Interchange	The state where the Interchange Authority has received the Interchange information (initial or revised).
Asynchronous	A two-part communication, involving a request message followed by a separate response message.
Author Rights	The rights a Request author has to submit, view, receive updates regarding, request changes to, and withdraw a Request.
Balancing Authority (BA)	A function associated with an electrical system bounded by interconnection (tie line) metering and telemetry.
Balancing Authority Area (BAA)	The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load resource balance within this area.
Base Profile	The profile associated with the new e-Tag, as originally requested.
Block Start Time	See Tag Start Time
CANCELLED	Final Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of CONFIRMED prior to the e-Tag's ramp start time with the termination time in the Request set to the block start time of the e-Tag and the Request State becomes APPROVED. The Authority sets the market level and transmission allocation of the e-Tag to zero. Once reached, this state may not transition to any other state.
COMMFAIL	A Delivery State indicating that communications were unable to be established between the sender of a message and the recipient.
Composite State	This is the overall state of the e-Tag which can have any of the following values: CONFIRMED, IMPLEMENTED, TERMINATED, CANCELLED, PENDING, WITHDRAWN, TERMINATED, EXPIRED and DENIED.
CONFIRMED	The Composite State of a tag for which the tag creation request is in a state of APPROVED, the ramp start time is greater than or equal to the current time, and which has not been CANCELLED or TERMINATED. This State may transition to IMPLEMENTED, CANCELLED, or TERMINATED.
Correction	A change to a Request e-Tag's composition prior to the expiration of the approval window, as defined in NERC/NAESB standards.
Current Level	The current level is derived based upon all approved e-Tag Requests applied in RequestID order. The current level represents the intended energy transfer at specific points in time. The initial current level is set to the market level for each base profile. The current level will vary by physical segment under certain circumstances ("in-kind" losses for example). The current

	level may be modified by either approved market level changes or reliability limit changes. The current level is set to the lower of the Exception Reliability Limit or the Effective Market Level which is defined as the current Exception Market Level if one exists or, if none exists, then the Base Market Level.
DC Tie Operator	An entity that operates a DC transmission facility; specifically, one that provides a connection between two different interconnections.
DELIVERED	Delivery State indicating that a particular Request was distributed to and received by a party.
Delivery State	A value used to provide information about a party's receipt of a particular Request.
DENIED	Approval State indicating that a party is unwilling to implement a particular Request. If one or more Approval Entities set their Approval State to DENIED then the resulting Request State will become DENIED upon the expiration of the Request's approval window. Once a Request achieves this state, it cannot transition to any other state.
Electric Industry Registry	Data set provided by the Electric Industry Registry vendor describing entity information, such as name, acronym, phone numbers, service URLs, etc… of registered participants.
e-Tag	Document describing a physical interchange transaction and its associated participants. An e-Tag is the result of one or more requests.
Exception Profile	A profile containing time specific changes to original profile values
Exchange	Amount of energy exchanged between two parties; encompasses both physical interchange and title transfers.
EXPIRED	Approval State and Request State that results when one or more reliability Approval Services fail to actively respond to the IA's assessment distribution before the assessment period ends. Once a Request transitions to this state, it cannot transition to any other state.
Financial Path	Path defining the financially responsible parties of a transaction, detailing ownership of energy across physical movement of energy as well as purely financial.
Generation Providing Entity (GPE)	Merchant selling energy from owned, affiliated, or contractually bound generation.
Implement	Allow energy to be scheduled as described.
IMPLEMENTED	The Composite State of a tag for which the tag creation request is in a state of APPROVED, the ramp start time is less than the current time, and which has not been cancelled or terminated. This State

	may transition to TERMINATED.
In-Kind Losses	Transmission losses delivered coincident with energy delivery.
Individual Approval State	The Approval State associated with a specific party to the e-Tag.
Individual Delivery States	The Delivery State associated with a specific party to the e-Tag.
Interchange Distribution Calculator (IDC)	NERC tool used to determine curtailments during TLR.
Interchange Transaction	A business exchange between two parties that result in the physical flow of energy from one point to another; a strict definition would indicate that exchange must be from one Balancing Authority to another, but for the purposes of this document, **any** such flow utilizing Point-to-Point service shall be considered an Interchange Transaction.
INVALID	Delivery state indicating that a party received a request distribution, but felt it was not syntactically or semantically correct
Load Serving Entity (LSE)	Marketer purchasing energy with the intent to deliver to and serve an affiliated or contractually bound load.
Market Entity	PSE, GPE, or LSE
Market Level	Desired energy profile for the transaction; level of market-desired flow.
Maximum Reservation Capacity	The commitment of transmission resources to support a particular transaction; typically the same as actual flow.
Minute Boundary	Date/Time value “seconds” are zero.
NA	Special Approval State or Approval State Type indicating that the entity does not have approval rights over the Request or that the Request has not yet been delivered to the entity.
OVERRIDE	Approval State Type indicating the Approval State for the entity was manually overridden by the entity providing the Authority Service.
PASSIVE	Approval State type indicating that the entity was unable to state their intentions within the assessment period and the system has made an automated decision on their behalf.
Passive Approval	An approval that occurred through the expiration of a Request’s evaluation window without an active approval; set automatically by the Authority when the expiration occurs. Passive approval is only applicable to non-reliability entities such as GPE, LSE, and PSE (whose transmission rights are cited).
Passive Denial	A denial that occurred through the expiration of a Request’s evaluation window without an active approval or denial; set automatically by the Authority when the expiration occurs. Passive

	denial is only applicable to reliability entities such as BA, SE, and TSP.
PENDING	Initial Request State and Approval State.
Physical Path	The source to sink route (via intermediate transmission paths) between generation and load.
Profile	A time/level matrix that defines an energy flow or other related information.
Purchasing-Selling Entity (PSE)	Any entity eligible to apply for an order requiring a Transmitting utility to provide Transmission Services under Section 211 of the Federal Power Act.
QUEUED	Delivery State indicating the Request is scheduled for delivery but has not yet been successfully delivered.
Ramp Start and Stop Times	The times determined using the e-Tag Start and Stop times in conjunction with the supplied or default ramp durations using the methodology defined in this specification.
Reliability Authority Service (RAS)	Service used to collect transaction information for analysis, particularly with regard to system security.
Reliability Coordinator (RC)	An entity that provides the reliability assessment and emergency operations coordination for a specific portion of an interconnection.
Reliability Entity	BA, SE, or TSP
Reliability Level	Profile at which a transaction may flow, based on reliability considerations; limit of energy flow.
Request	An electronic notation of a particular desired action with regard to a new or existing interchange transaction. An APPROVED Request results in either the creation of an e-Tag or the modification of an existing e-Tag.
Request For Interchange (RFI)	A collection of required data, as defined in Appendix C of the NAESB Coordinate Interchange standard, necessary for the purpose of submitting to the Interchange Authority as an Arranged Interchange.
Request State	The overall status of a Request which can be any of the following: PENDING, APPROVED, WITHDRAWN, EXPIRED, or DENIED.
Scheduling Entity (SE)	Scheduling Entity – Reference in the e-Tag for the Balancing Authority responsible for the bulk transmission system over which a transmission segment flows. The SE may also be an entity performing this function on behalf of the Balancing Authority and must be defined as performing that function in the Electric Industry Registry.

Security Key	A security token, used to authenticate an entity involved in the e-Tag messaging system
Service	One of four types of computer systems used in the e-Tag messaging system (Tag Agent, Authority, Approval, Reliability Authority)
Sink	Final point of delivery for a transaction.
Sink Balancing Authority (Sink BA)	The Balancing Authority metered area in which load is located
Source	Initial point of supply for a transaction.
Source Balancing Authority (Source BA)	The Balancing Authority metered area in which generation is located.
State	Either the Request State, Composite State, Individual Delivery State, or Individual Approval State.
Straddle Ramp	Ramp that divides the start ramp duration equally across the profile block start or end time.
STUDY	The approver has actively decided to defer their decision to approve or deny until a later time within their approval window, but wishes to communicate their acknowledgement of the request back to the sender.
Synchronous	Message type in which the requesting message is responded to within the same connection.
Tag	e-Tag
Tag Agent Service (Agent)	Software component used to generate and submit new e-Tags, Corrections, and Profile Changes to an Authority and to receive State information for these requests.
Tag Approval Service (Approval)	Software component used to indicate individual approval entity responses when requested by Authority Service, as well as submit Profile Changes.
Tag Author	Entity that creates and submits an e-Tag; the caller of the Request NewTag method.
Tag Authority Service (Authority)	Software component that receives Agent and Approval Requests and Responses and forwards them to the appropriate Approval Services. Also maintains master copy of an e-Tag (all associated Requests), the Composite State of the e-Tag, etc. and responds to queries regarding the e-Tags in its possession
Tag Code	7 Character code used as part of the e-Tag ID to identify a transaction.
Tag ID	Identifier of the e-Tag represented by combining Source BA code, PSE code, an e-Tag Code, and Sink BA code.

Tag Start Time	The earliest time listed in any part of a tag, including energy, transmission, and loss accounting.
Tag Stop Time	The latest time listed in any part of a tag, including energy, transmission, and loss accounting.
TERMINATED	Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of IMPLEMENTED. The termination time plus stop ramp duration must be greater than or equal to the current time. The Authority sets all market level and transmission allocation profiles of the e-Tag to zero at and after the termination time when the Request State becomes APPROVED. Once an e-Tag has reached this Composite State, it cannot transition to any other Composite State, and the e-Tag can only be adjusted between its block start time and the Request's termination time (i.e. it can no longer be extended past the Request's termination time).
Test e-Tag	An e-Tag used for diagnostic purposes; does not represent actual transacted business.
Title Transfer	An exchange of energy ownership; may or may not be associated with a physical movement of energy.
Transaction Information System (TIS)	Transaction Information System – currently implemented as e-Tagging.
Transmission Allocation	Set by the e-Tag Author, it is a description of how a reservation or contract is being used in a particular e-Tag. The Transmission Allocation allows the author to specify the duration and megawatt level of the capacity used from a transmission reservation to support the e-Tag transaction.
Transmission Customer (TC)	A PSE specified as owner (rights holder) in a Transmission Allocation in the e-Tag. The PSE may or may not be the energy title holder.
Transmission Service Provider (TSP)	A registered entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
Universal Coordinated Time (UTC)	Time standard used by the e-Tagging System for communication purposes; also referred to as Greenwich Mean Time (GMT).
Valid	Passed syntax checks by an e-Tag Service (i.e. not invalid)
Viewing Rights	The rights of an entity to view transaction details.
WITHDRAWN	Final Request State that results when a request submitter (Tag Author or Adjustment requester) submits a WithdrawRequest message before the Request has reached any other final state (e.g.,

	APPROVED, DENIED, etc.). This state may not transition to any other state.

1.3 Tagging Terminology

In an abstract sense, Electronic Tagging's primary purpose is to create, manipulate, and maintain two objects – e-Tags and Requests. An e-Tag can be thought of as a collection of Requests, bundled together in one package and relating to a single transaction. Requests can be of various types, and each Request contains its own state and approval history. Each approved Request modifies the e-Tag that it is associated with in some way. E-Tags also maintain their own state (called Composite State), independent from the states of the various Requests that make up that e-Tag.

References to "time" in this document mean a specific date/time in most cases; e.g. ramp start time, ramp stop time, e-Tag start time, etc.

The remainder of this section contains a list of useful terms and definitions relating to e-Tags and Requests.

Request - New e-Tags and changes to existing e-Tags are all initiated with a Request. An e-Tag is the composite result of all APROVED Requests related to that e-Tag. There are six types of requests:

New e-Tag – a request to implement a new Interchange Transaction as a physical energy flow, also called a Request for Interchange. An e-Tag that reaches an IMPLEMENTED state will usually transition through the following stages:

1. Request for Interchange – the Request created by the e-Tag Author.
2. Arranged Interchange - once the Authority receives the Request.
3. Confirmed Interchange - once the Request is approved.
4. Implemented Interchange – when the current time is past the e-Tag's ramp start time.

Curtailment – a request to limit an energy flow through the limiting of an associated Interchange Transaction
Reload – a request to release a limit previously requested through a Curtail Request
Adjustment – a Request that modifies energy flow and/or transmission capacity of an Interchange Transaction in order that such a change may be implemented and resources committed
Termination – a Request that either reduces energy flow and transmission capacity of an e-Tag to zero for the life of the e-Tag prior to its start so that such a transaction is not started (CANCEL) or reduces energy flow and transmission capacity of an e-Tag to zero starting at a time indicated in the termination Request that is after ramp start time and continuing for the life of the transaction (TERMINATION)

Extension – a Request that includes energy flow and/or transmission capacity for unscheduled hours of an Interchange Transaction, in order that such a change may be implemented and resources committed

Submission time – the time at which an e-Tag Author submits a Request to the Authority for processing *as determined by the Authority*. Requests are categorized by submission time into one of three categories based on the NERC/NAESB Interchange Standards' timing tables. These categories are:

1. On Time,
2. Late, and
3. After The Fact (ATF).

Request State – the overall status of the Request, based on the processing of the Request. Requests are categorized by Request State in the following ways:

PENDING - initial Request State

WITHDRAWN – final Request State that results when a Request Author submits a WithdrawRequest before the Request has reached any other final state (e.g., APPROVED, DENIED, etc.). This state may not transition to any other state.

APPROVED – final Request State that results when all entities with approval rights over a Request actively approve it or when no entities with approval rights actively deny the Request, all reliability entities approve the Request, and the Request's assessment period expires.

DENIED – final Request State that results when one or more Approval Entities set their Approval State to DENIED and the Request's assessment period expires.

EXPIRED – final Request State that results when one or more reliability Approval Services fail to actively respond to the IA's assessment distribution before the assessment period ends. Once a Request transitions to this state, it cannot transition to any other state.

Individual Delivery States – indicates the successful or unsuccessful transfer of a Request to an entity. The possible Delivery States are:

QUEUED – the Request is scheduled for delivery.

INVALID – the Request was perceived as invalid by the receiving entity and rejected.

COMMFAIL – the Request was undeliverable due to communication problems.

DELIVERED – the Request was successfully delivered.

Individual Approval States – indicates the intent of an entity to implement a Request. The possible Approval States are:

NA – no state is applicable, as the Request has not yet been successfully delivered to the entity or the entity does not have approval rights.

PENDING – no indication has been made to show whether the implementation of the Request is supported or not.

APPROVED - an indication of supporting the implementation of the Request.

DENIED - an indication of opposing the implementation of the Request.

STUDY - an indication that the Approval Entity was uncertain whether or not to support or oppose the Request. This state is treated the same as PENDING when the assessment period ends.

EXPIRED – an indication that an Approval Entity who is required to actively set Approval State did not actively set Approval State to APPROVED or DENIED before the assessment period ended.

Individual Approval State Types – indicates how an entity's state was assigned. The possible Approval State Types are:

Active – an Approval Entity actively selected The Approval State.

Passive – the Approval State was passively selected due to a time elapse or other non-interactive manner.

Overridden – the Approval State was actively selected by the Sink Balancing Authority via its Authority Service acting on the behalf of an Approval Entity that was unable to act on their own.

Composite State Types – indicates the overall state of an e-Tag. The possible Composite States are:

CONFIRMED –Composite State of an e-Tag that results when the new e-Tag's creation Request is in an APPROVED state and the e-Tag ramp start time is greater than the current time.

IMPLEMENTED – Composite State of an e-Tag that results when the new e-Tag's creation Request is in an APPROVED state and the e-Tag ramp start time is less than or equal to the current time.

CANCELLED – Final Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of CONFIRMED with the termination time in the Request set to the block start time of the e-Tag. The Authority sets the market level and transmission allocation of the e-Tag to zero. Once reached, this state may not transition to any other state.

TERMINATED – Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of IMPLEMENTED with the termination time set after the block start time of the e-Tag. The termination time plus stop ramp duration must be greater than or equal to the current time. The Authority sets all market level and transmission allocation profiles of the e-Tag to zero at and after the termination time when the Request State becomes APPROVED. Once an e-Tag has reached this Composite State, it cannot transition to any other Composite State, and the e-Tag can only be adjusted between its block start time and the Request's termination time (i.e. it can no longer be extended past the Request's termination time).

PENDING - Initial Composite State

WITHDRAWN – The e-Tag Composite State transitions to WITHDRAWN when the new e-Tag creation Request transitions to WITHDRAWN.

DENIED – The e-Tag Composite State transitions to DENIED when the new e-Tag creation Request transitions to DENIED.

EXPIRED - The e-Tag Composite State transitions to EXPIRED when the new e-Tag creation Request transitions to EXPIRED.

1.4 System Concepts

The functional requirements address the following basic information and data exchange needs:

- Initial creation of an e-Tag Request representing the transaction,
- Dissemination of the e-Tag Request to all parties directly involved in the transaction,
- Collection of Approval States from all parties with approval rights,
- Forwarding of the Request and e-Tag to appropriate entities and tools, and
- Modifications to the e-Tag throughout its lifetime.

This document approaches the functional requirements for electronic Tagging by defining four services: the Agent Service, the Authority Service, the Approval Service, and the Reliability Authority Service.

The functionality that must be supported by each of these services and the entity responsible for providing for these services are defined. There are no restrictions with regard to who may provide these services (i.e., the responsible entity or any one of a number of third-party service providers) nor any restrictions on which services (or all) that a third-party service provider could offer. **Under no circumstances shall a provider of any of these services require any other service provider to implement additional features or functionality beyond these specifications as a condition to properly performing the obligations associated with that service.**

1.4.1 System Architecture

1.4.1.1 Agent Service

The Agent Service provides the ability for initial creation of an electronic e-Tag and the transfer of that information to the appropriate Authority Service. Purchasing-Selling Entities (PSEs) and all other e-Tag Authors are responsible for providing this service directly or by arranging with a third party to provide this service as their agent. E-Tags created by the Agent Service are forwarded to the Authority Service associated with the Sink Balancing Authority (Sink BA). The Agent Service provides a mechanism for the e-Tag Author to view the Approval State of its transactions via an unsolicited notification mechanism. The Agent Service also provides facilities for the e-Tag Author to make Corrections to e-Tags prior to confirmation, as well as request a Profile Changes to any of their e-Tags following confirmation. These corrections and modifications are also sent and processed via the Authority.

The Agent Service is referred to throughout this document as **Agent.**

1.4.1.2 Authority Service

The Authority Service is the focal point for all interactions with an e-Tag and maintains the single authoritative “copy of record” for each e-Tag received. Every Sink Balancing Authority is responsible for providing this service directly or by arranging with a third party to provide this service as its agent. The Authority Service forwards all valid received e-Tag Requests to the Approval Service associated with each entity identified in the transaction as having “approval” or “viewing” rights over that Request, and collects approvals/denials issued by these Approval Services. Based on time and/or the messages received from the Approval Services, the Authority arbitrates and sends the final disposition of the Request to the originating Agent and all Agent and Approval Services associated with the transaction, and to the sink BA’s designated forwarding location (e.g., RAS or BA’s Reliability Coordinator). The Authority Service also provides the capability for both Agent and Approval Services to interrogate the current Approval State of any transaction request on demand.

The Authority Service is referred to throughout this document as **Authority.**

1.4.1.3 Approval Service

The Approval Service receives e-Tag Requests submitted by Agents via the appropriate Authority. The Approval Service also provides a means for an entity to receive notification of transactions in which they are involved, as well as send approve or deny responses to an Authority's presentation of a valid Request (if they have approval rights over the Request). Additionally, the Approval Service allows entities to curtail or otherwise modify the profile of an existing e-Tag (if they have rights to do so). Balancing Authorities, Transmission Service Providers, and Purchasing-Selling Entities are responsible for providing this service directly or for arranging with a third party to provide this service as their agent. Finally, Transmission Service Providers may use the Approval Service to issue corrections or adjustments.

The Approval Service can be referred to throughout this document as **Approval.**

1.4.1.4 Reliability Authority Service

Reliability Authority Services receive all Requests from Authorities. These e-Tags inform the Reliability Authority Service of the expected flows a transaction will create, and are used by Reliability Coordinators to mitigate constraints should the need arise.

The Reliability Authority Service can be referred to throughout this document as **RAS.**

1.4.2 Tag Identification

All e-Tags and e-Tag creation Requests shall be uniquely identified by an e-Tag ID. Electronic communications between Agent, Authority, and Approvals shall require the association of an additional Security Key or Keys to control all interactions related to a given transaction. The following subsections describe the requirements for the creation of the e-Tag ID and Security Key.

1.4.2.1 E-Tag IDs

Every transaction shall be identified by a unique e-Tag ID based on key attributes of the transaction as specified in the Data Model:

- Source Balancing Authority Code
- PSE Code (Tag Author PSE)
- Unique transaction identifier
- Sink Balancing Authority Code

The "Source Balancing Authority" shall be defined as the host Balancing Authority in which the generation is located. The "Sink Balancing Authority" shall be defined as the host Balancing Authority in which the load is located. The "e-Tag Author PSE" shall be defined as the PSE who is creating and submitting the new e-Tag Request to the Authority.

Since this e-Tag ID and the contents of the e-Tag contain potentially commercially sensitive information, all components of the e-Tagging Information System shall treat such information as confidential.

All services shall reject any attempt to submit as new an e-Tag ID that is identical to an existing e-Tag creation Request's e-Tag ID for a period of one (1) year from the stop date and time associated with the existing e-Tag. Agents shall be required to ensure that each e-Tag ID is unique for a period of not less than one (1) year from the stop date and time associated with the last transaction that was assigned that e-Tag ID.

1.4.2.2 Security Keys

The electronic exchange of e-Tag information shall require the assignment of unique "Security Keys" to be associated with the transaction. Security Keys control communication between the Agent, Authority, Approval, and RASs.
The Security Key is a unique 12 character alphanumeric (0–9, A–Z, a–z; case sensitive) security token.

The Agent generates a unique Security Key to associate with the e-Tag at the time of submission. All subsequent messages exchanged between the Agent and the Authority in regard to the e-Tag shall refer to both the e-Tag ID and Security Key assigned by the e-Tag Author's Agent.

The Authority shall also generate unique Security Keys to be associated with the e-Tag on the initial transmission of the e-Tag to each of the appropriate Agents or Approvals. All subsequent messages exchanged between the Authority and a given Approval in regard to the e-Tag shall refer to both the e-Tag ID and Security Key assigned by the Sink Balancing Authority's Authority.

In certain situations, Security Keys can exist independent of e-Tag IDs (such as the Get e-Tags and Get e-Tag IDs requests). Those situations will be described in detail in the appropriate sections of this document.

The Security Key must either be random or have the appearance of randomness. Although schemes may be used to generate a key, these schemes must not be obvious to the interested observer (for example, APR05991240X is obviously a date and time, but a ciphered version of this, KYZ71434450H, might not be). The Security Key must be considered a security mechanism, and as such, must not be easily deducible by parties lacking first-hand knowledge of the specific Security Key generation mechanism employed by the system.

It should be noted that each Authority is assigned by NERC a unique Security Key for interaction with the IDC. This key is only to be used for communication with the IDC, and must be kept confidential. This key secures communications from the IDC to each Authority as well. NERC will notify each registered Authority with that Authority's unique Security Key to be used in all messages between the IDC and Authority.

1.4.3 Test e-Tags

Test e-Tags are e-Tags used for the purpose of troubleshooting a system or component of the system. All services (Tag Agent, Authority, and Approval) shall accept and process Test e-Tags and in an identical fashion to all other e-Tags, with the following exceptions:

- Viewing applications MUST indicate to the user that the e-Tag is a Test e-Tag.
- Test e-Tags do not require an approving party to evaluate the e-Tag within the Assessment Time as defined in NERC/NAESB Standards.
- Test e-Tags must not be treated as actual e-Tags (the information contained within a Test e-Tag must not be used to make any business decisions).
- The Authority shall not initiate the forwarding of these test e-Tags to the RAS at any time.
- Test e-Tag Requests always transition to a Request State of APPROVED on expiration of the assessment period and no approval entities have denied the Request or when all approval entities have approved the Request.

In addition, the following rules must be observed with regard to test e-Tags:

- Test e-Tags must ONLY be used for troubleshooting purposes. System Development, Training, and Demonstration, as well as any other non-troubleshooting related need must NOT utilize the Test e-Tag feature.
- A particular PSE (as listed in the Electric Industry Registry) may only issue a total of ten (10) Test e-Tags per clock hour. Any Test e-Tag submissions exceeding this number may be rejected at the option of the service being sent the Test e-Tag.
- Test e-Tags may be rejected at the option of the service provider if they are sent during the last twenty minutes of a clock hour (i.e., xx:40 – yy:00).
-

Test e-Tags must not reflect authorship that does not match the listed service affiliation in the Electric Industry Registry. If a Test e-Tag is sent from an external system to another system, and the e-Tag Author is a registered user of the receiving system, the receiving system may reject the e-Tag. For example, if PSE XXX is registered to use vendor X, and a message comes in from vendor Y claiming to be authored by PSE XXX, vendor X may reject the message.

1.4.4 Communications

All e-Tag messages are sent using the SMXP (Simple Method Exchange Protocol). This protocol is based upon a *remote procedure call* paradigm. This means that instead of sending messages explicitly, procedures on remote machines are invoked, passing any needed data as input parameters to the function or method. When the function is complete, it returns the result of its processing.

1.4.4.1 Method Types

E-Tag uses various types of methods for various purposes. The methods can be broken up into the following categories.

1.4.4.1.1 Requests

A request method is any method that initiates an action associated with a transaction. Such actions include e-Tag submission and adjustment.

1.4.4.1.2 Request Distributions

Request Distributions are the methods used to send requests to all entities impacted by the e-Tag. Request distributions may be informational, or may indicate a requirement for approval.

1.4.4.1.3 Actions

Actions are those methods that directly set a value. These methods include request approval, denial, and withdrawal.

1.4.4.1.4 Information Distributions

Informational distributions are the methods used to send information related to the State of a particular Request or set of transactions. These are sent to entities to alert them of particular Request's implementation or withdrawal, as well as specific entities approvals and denial of a Request.

1.4.4.1.5 Queries

Query methods are used to search and recover data from an Authority or similar service. Most query methods use parameters that allow the server to filter unneeded data and return the smallest reply message possible. Which parameters may be specified depends upon which query method is called. Many queries are asynchronous methods, meaning the results of the query will return via a callback. Others are synchronous, meaning the response contains the results of the query.

1.4.4.1.6 Callbacks

Callbacks are methods that are used to return results from asynchronous queries. Each callback will be associated with a previously called query that was used to create the result set.

1.4.4.2 Message Size Limitations

In order to ensure reliable operation of the e-Tag systems, the following limitations of message size are to be observed:

- Any RequestNewTag or RequestProfileChange specifying a duration greater than 33 days in length may not have a Content-Length greater than 512000 characters. Agent systems should not issue such Requests, and Authorities should reject such Requests if they are received.

1.4.5 Financial and Physical Paths

Paths define the flow of both energy flow and fiduciary responsibility. Financial path components are referred to as **market segments**, while physical path components are called **physical segments**.

A Physical Segment may be one of three types:

- **Generation** that is supplying energy for delivery,
- **Transmission** that is wheeling the energy from one point to another, and
- **Load** that is consuming the delivered energy.

Market Segments are financial responsibilities for the receipt and/or delivery of the energy. A Market Segment typically contains Physical Segments (illustrating holding of title across physical movement of energy), but may contain no such Physical Segments (illustrating a non-physical title-holder). Physical Segments must be contained within Market Segments.

An e-Tag may have only one Generation segment and one Load Segment. When ordered, these segments must be indicated as the first and last physical segments in the path, respectively.

For a detailed discussion of Paths and how they function, please see **Section 6.2.2, Market Segments**, and **Section 6.2.3, Physical Segments.**

1.4.6 Profile Descriptions

Profile Sets define the level at which transactions should run, as well as the factors that set those levels. For detailed discussions on how profiles function please see section **6.1.4.**

In general, a profile will have three levels

- The energy flow
- The maximum level at which the energy may reliably flow (default is unlimited)
- The transmission capacity committed to the transaction by the e-Tag Author as a Transmission Allocation

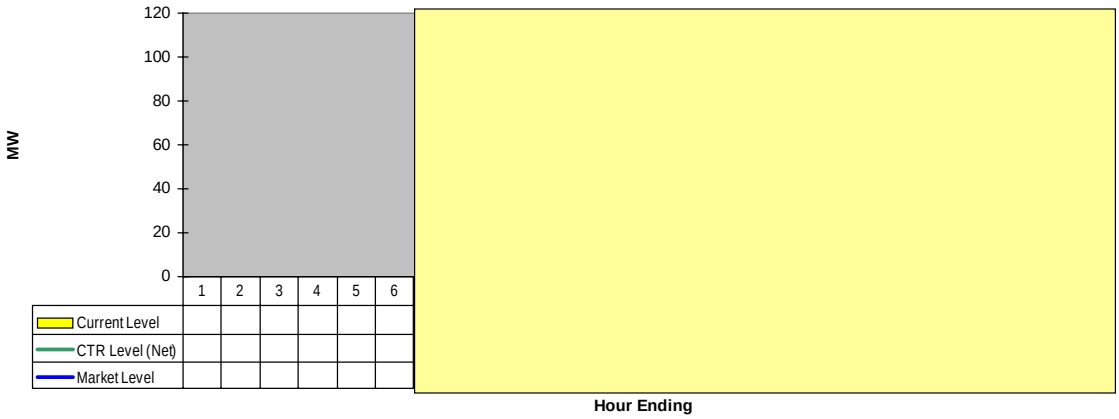
Tag Authors can modify the energy profile up or down without exceeding the Transmission Allocation. Should a curtailment occur for reliability reasons, then the reliability limit must be adjusted to become the new maximum level. The e-Tag Author can modify the energy profile on the e-Tag up or down even while under curtailment, but the reliability limit will always be the maximum level. The lowest of the reliability limits or the market level will indicate the actual flow on the e-Tag. .

Profiles may optionally reflect ramp start and stop durations for each profile block. The ramp stop duration will be ignored on all blocks except for the last profile block. Only the ramp start duration will be used in energy level calculations for all other profile blocks. All ramps imply straddle ramps. Instantaneous ramps are indicated by a zero minute ramp duration. The ramp start and stop data represents minutes over which the generator will increase or decrease generation from the previous block level to the current block level. The ramp beginning and end times for each profile block can be calculated based on the ramp duration and profile block start and end times.

The following diagrams illustrate the relationship between these levels:

STEP 1 – New Tag Submission

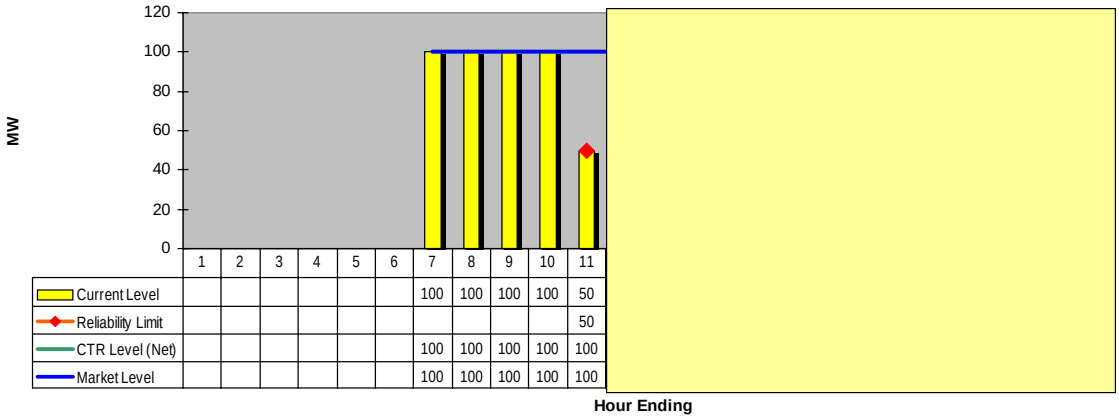
HE7 - HE22 100MW



In Step 1, the e-Tag has been submitted, but has not yet run. The yellow overlay indicates points in the future.

STEP 2 – Curtailment

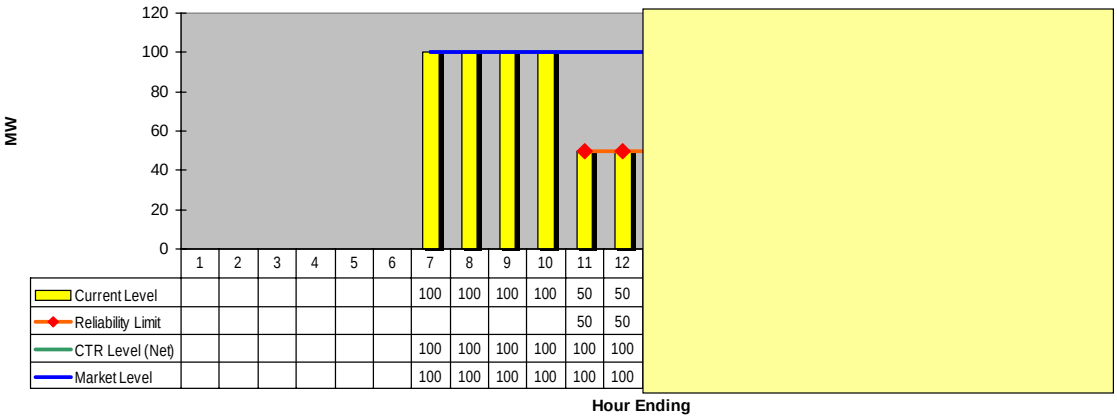
Curtailed to 50MW at 10am



In Step 2, the e-Tag has been running and is curtailed.

STEP 3 – Curtailment Continues

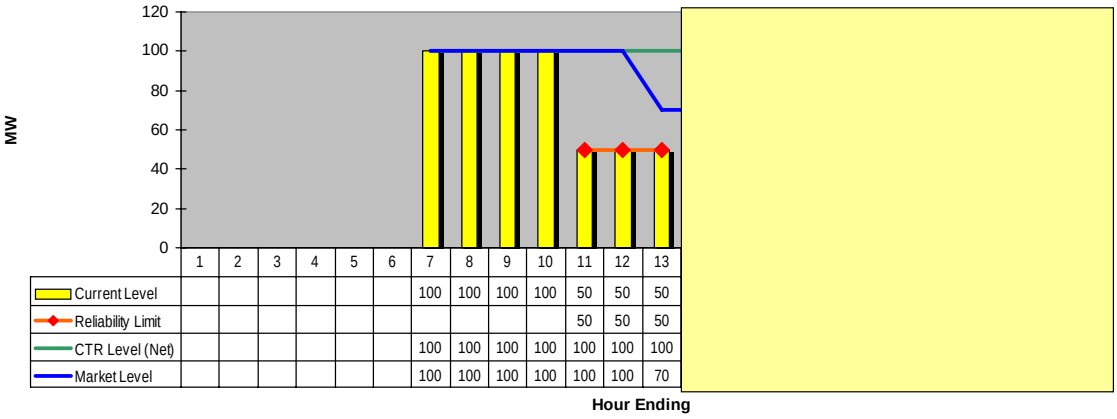
Reissued at each hour



In Step 3, the Curtailment continues and is reissued twice.

STEP 4 – Tag Author Sets Reload Level

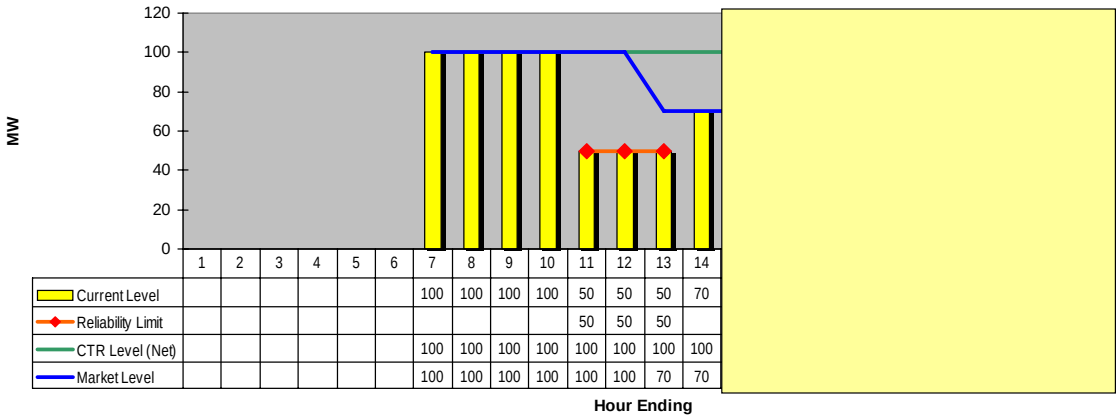
70MW until HE 18



In Step 4, the e-Tag Author elects to limit their transaction to a maximum reload of 70MW until HE 18.

STEP 5 – TLR Released, Tag Partially Reloaded

Relaoded to 70MW

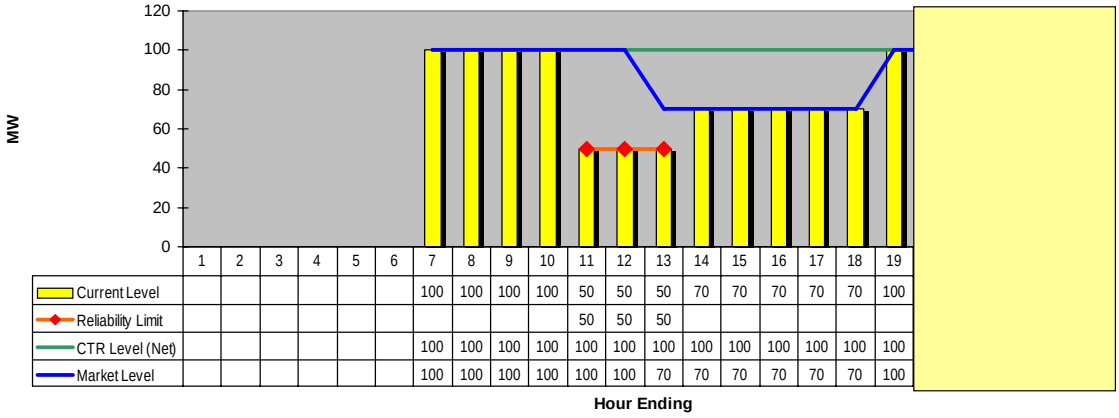


	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Current Level							100	100	100	100	50	50	50	70
Reliability Limit											50	50	50	
CTR Level (Net)							100	100	100	100	100	100	100	100
Market Level							100	100	100	100	100	100	70	70

In step 5, the e-Tag is Reloaded by the RC/BA to the 70MW level as specified.

STEP 6 – Tag Fully Reloaded

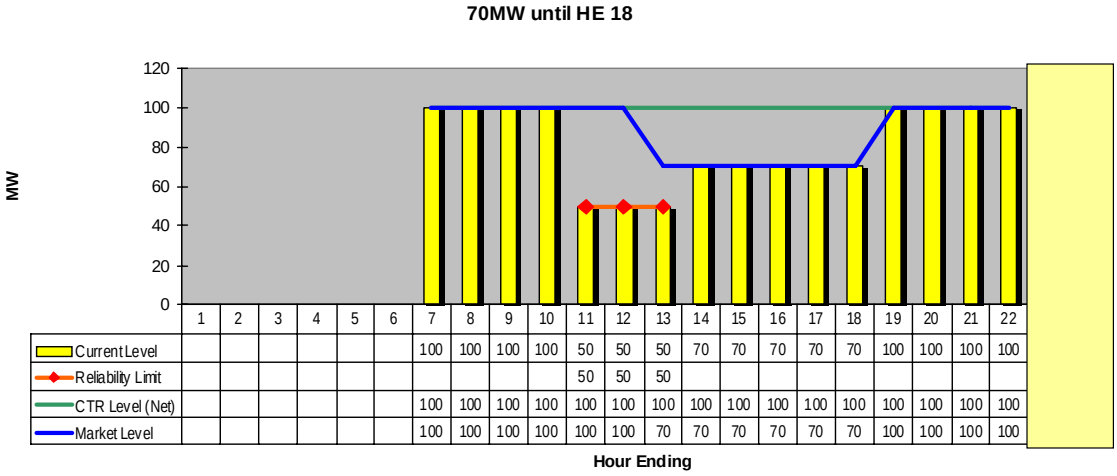
70MW until HE 18



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Current Level							100	100	100	100	50	50	50	70	70	70	70	70	100
Reliability Limit											50	50	50						
CTR Level (Net)							100	100	100	100	100	100	100	100	100	100	100	100	100
Market Level							100	100	100	100	100	100	70	70	70	70	70	70	100

In Step 6, the e-Tag is reloaded by the RC/BA to its previous 100MW level as specified.

STEP 7 – Transaction Complete



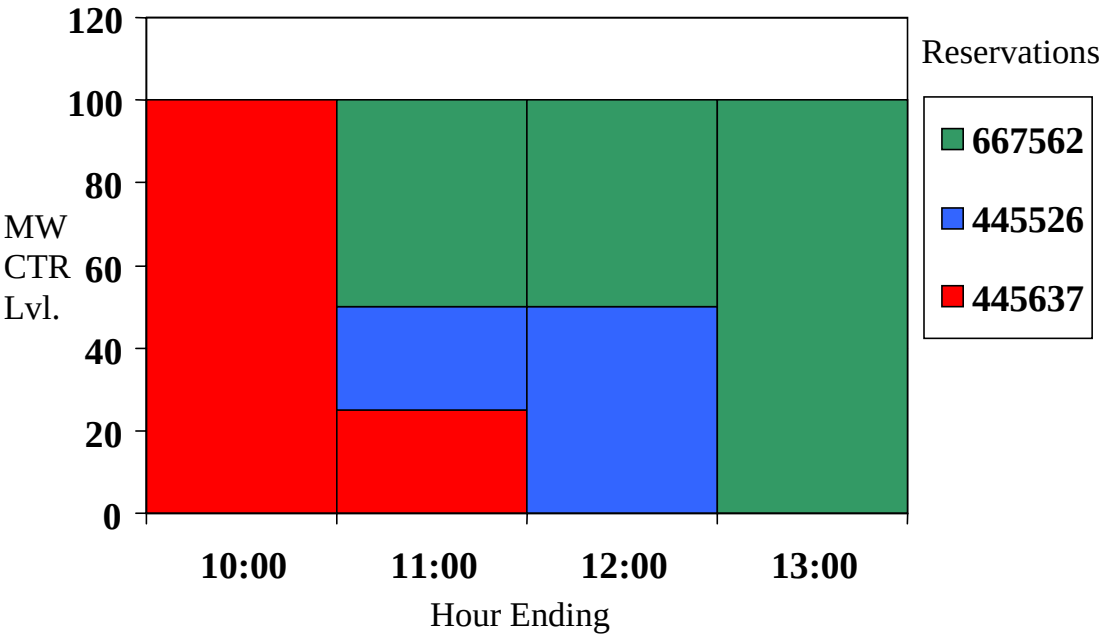
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Current Level							100	100	100	100	50	50	50	70	70	70	70	70	100	100	100	100
Reliability Limit											50	50	50									
CTR Level (Net)							100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
Market Level							100	100	100	100	100	100	70	70	70	70	70	70	100	100	100	100

In Step 7, the e-Tag has completed.

1.4.7 Transmission Allocation

Transmission Allocation describes the manner in which an e-Tag Author specifies which transmission reservations will be used to support the capacity committed in a Transmission Service Provider's associated profile. The Transmission Allocation allows the author to specify the duration and megawatt level of the capacity used from a transmission reservation to support the e-Tag transaction.

In the example below, an entity is supplying a total of 100 MW of transmission capacity over four hours by using three different reservations in combination:



For more detail on this topic, please see **Section 6.2.4, Transmission Allocations**.

1.4.8 Timing Requirements

To enforce Request submission and evaluation timing requirements, the Authority shall maintain system time to an accuracy of one (1) second traceable to the National Institute of Standards and Technology (NIST). Approval and Agents are encouraged to keep their time synchronized in this manner as well.

All times communicated through an e-Tag shall be noted in Universal Coordinated Time (UTC). User interfaces and local systems may reflect local time, however, any system using time zones other than UTC must properly convert those times into UTC prior to communicating with other systems.

NERC/NAESB Standards provide details on the manner in which timing requirements should be implemented.

1.4.8.1 Approval of Reliability Changes

All profile changes that impact Reliability Limits (i.e., curtailments and reloads) must be actively approved in order to be implemented. Profile changes will not be implemented if either actively or passively denied.

1.4.9 Tag Auditing

Each service shall be responsible for keeping audit information describing its interactions with other services. These requirements are described below.

1.4.9.1 Message Rejection Log

Any service that rejects a message as containing a Fault or an Error must log the type of rejection, the date/time of the rejection, the sending entity (if identifiable), and the e-Tag ID (if identifiable). This information must be kept available by written request for a minimum of ninety (90) days after the rejection.

1.4.9.2 Historical e-Tag Archive

Every service shall keep available for retrieval every e-Tag and associated messages received by the service until ninety (90) days past the e-Tag's stop date/time. Authorities must have this information available to Approval and Agent systems through standard e-Tag querying mechanisms throughout the ninety-day period, as well as through written request by other parties who may require data but not be participants listed on the e-Tag (i.e., NERC).Agent and Approvals must have these e-Tags available by written request. Approval and Agent systems making a request from the Authority for a certain time range must be provided with all e-Tag and associated messages associated with the requestor for that time range.

1.4.9.3 Statistics

Every service shall maintain statistical information as defined below. This information must be logged, as it occurs, NOT after the fact. In this manner, services may accurately reflect data before it is modified through overrides or updates. This information must be available by written request for a minimum of ninety (90) days in the form or reports. These reports must be written based on the requests processed in one week (00:00 UTC Sunday to 23:59:59 UTC Saturday). This information must be available to parties who may require data but not be participants to any specific e-Tag (i.e., NERC).

- Number of LATE Requests, by requester
- Number of ATF Requests, by requester
- Number of return values of INVALID, by entity
- Number of return values of COMMFAIL, by entity
- Number of returned Faults, by entity.
- Number of Request Approval State Type of PASSIVE, by approver

1.4.9.4 Authority Off-Line Archive

All Authorities shall archive all message dialogues (all received and issued messages and their associated responses) associated with a particular e-Tag. These message logs need not be available for online query, however, upon written request from NERC, Authority operators must be able to supply written reports within a reasonable amount of time (within one working week) listing message traffic for a particular entity or transaction.

This information shall be kept from the implementation of the 1.7 Specification forward until such time this requirement is removed.

1.4.10 Rounding

MW values specified in e-Tag profiles must sometimes be integrated into MWh values across appropriate schedule intervals. E-Tag profiles that start or stop within schedule intervals may result in fractional MWh values being calculated. These MWh values must be rounded to the nearest whole MWh (< .50 down, >= .50 up).

Calculation of aggregated data such as hourly, daily, monthly, and e-Tag totals must be performed in accordance with applicable NAESB/NERC Coordinate Interchange Standards.

1.4.11 Carbon Copy List

E-Tags may optionally contain a list of entities (BA, TSP, or PSE) that are provided with a copy of the e-Tag. This list is set as part of an e-Tag creation request and can't be changed by subsequent corrections, adjustments, etc. E-Tag Authors may select up to five entities for inclusion in this list. These entities are provided with a copy of the e-Tag and any subsequent changes in the same manner as which entities in the Market Path are provided with copies of the e-Tag. These entities will not be given approval rights and must not appear in any other role in the e-Tag. For entities of type PSE, all messages will be sent to the registered agent URL. For entities of type BA and TSP, all messages will be sent to the registered approval URL.

1.5 Training Requirements

1.5.1 User Guides

Anyone developing e-Tag software must provide a User Guide, which shall describe, at a minimum, the following information:

- The target user (Author, Approver, or Reliability Coordinator)
- e-Tag principles (to be based on the NERC/NAESB Standards and this specification)
- Software implementation of those principles (to be based on the developer's user interface)
- How those implementations are to be utilized
- How problems and errors can be resolved

1.5.2 User Education

Anyone developing e-Tag software must develop education programs for the use of their software. Education programs must cover the following topics:

- Who the target user is (Author, Approver, or Reliability Coordinator)
- e-Tag principles (to be based on the NERC/NAESB Standards and this specification)
- Software implementation of those principles (to be based on the developer's user interface)
- How those implementations are to be utilized
- How problems and errors can be resolved

Education programs may be developed for self-study, online education, or other means. The developer may offer education Workshops; however, the cost of such workshops may be borne by the software customer.

1.6 Functional Concepts

1.6.1 Initiating a Request

Requests are initiated in order to create or modify e-Tags.

1.6.1.1 Submitting a New e-Tag Request

Submitting a New e-Tag Request is the process in which an e-Tag Author presents a completed RFI/ e-Tag to the e-Tag system for processing. The e-Tag Author uses its Agent to write the e-Tag and then communicate that e-Tag as a request to the Authority. The Authority then processes the transaction and manages the state of the new e-Tag Request. Upon receipt, the Authority sets the ActOnByTime and the TimeClassification (OnTime, Late, or ATF) based on the time of receipt, the ramp start time of the RFI, and the NERC/NAESB Interchange Standard timing tables. A New e-Tag Request must specify a proper Base Profile, as described in section 6.1.4.2.1.

1.6.1.2 Submitting a Correction Request

The e-Tag Author makes e-Tag Corrections when a portion of the e-Tag data must be changed. A correction to an e-Tag can only occur prior to that e-Tag attaining a Composite State of CONFIRMED or IMPLEMENTED. During the New e-Tag Request approval process, in which parties evaluate the transaction for ability to implement, the e-Tag Author may notice or be informed of a needed change in the e-Tag. That change may be written and submitted using the Agent.
The correction resets the Request State for entities affected by the correction, distributes the correction, and requires entities affected to re-evaluate the Request using the corrected data. Upon receipt of a corrections submittal, the Authority resets the ActOnByTime and the TimeClassification based on the NERC/NAESB Interchange Standard Timing Tables. Unaffected entities need not re-approve the e-Tag. Affected entities are defined in section 1.6.2.2.

Transmission Service Providers (TSPs) may also submit a correction. In this case, the TSP is only allowed to modify the TransProductRef and transmission allocation on a physical segment where they are the associated TSP (TPCode). The TSP may horizontally or vertically stack transmission, just as the e-Tag Author can, however the total transmission allocation MWlevel may not be changed (either reduced or increased) and the profile may not be extended. TSP created Correction Requests are unilateral and require no approval by any other entity. Upon receipt of a corrections submittal from a TSP, the Authority does not reset the ActOnByTime or TimeClassification but will redistribute the correction.

NERC/NAESB Standards provide additional details on the manner in which corrections should be made.

1.6.1.3 Submitting a Profile Change Request

Profile Changes can be requested by several different parties and for three primary reasons:

- To implement market-based modifications to the Transmission Allocation profile.
- To implement market-based desires to modify or extend energy flow
- To implement reliability-based desires to modify energy flow (i.e., curtailments and reloads)

When any of the above possible Profile Changes are needed, the party wishing to implement the Profile Change will use their appropriate e-Tag service to write and send the change Request to the Authority. The Authority then processes the transaction and manages the state of the Request. When a profile change is requested for reliability purposes (i.e. curtailment or reload), the Request author must submit a modified profile at the POR or POD of any single physical segment; the Authority will then calculate the approximate losses for all other profiles, if applicable.
When an e-Tag Author requests a profile change, they must provide all appropriate profiles necessary to reflect appropriate losses.

1.6.2 Request Distribution

1.6.2.1 Distributing a New e-Tag Request

When an agent submits a new e-Tag request to an Authority, the Authority distributes copies of that e-Tag to the transaction's participants. Transaction participants include all entities specified in the physical and market path, entities selected in the carbon copy list, and any other entities as specified in the NERC/NAESB Interchange Standards. The rights associated with each participant are defined in NERC/NAESB Standards. Entities in the carbon copy list must not be given approval rights.

The Authority provides a copy of the new e-Tag to each participant, along with a description of their role in the transaction. Each receiving Approval then processes the Request and solicits approval of the Request from its using participant.

1.6.2.2 Distributing a Correction Request

Corrections are distributed to all entities that received the original e-Tag. Entities specifically impacted by the correction are asked to re-evaluate the e-Tag based on the corrected information. Impacts of corrections are defined in the following table.

Correction Type	Impacted Entity
Any allowable correction to a Physical Generation Segment	*Source BA, Generation Providing Entity*
Any allowable correction to a Physical Transmission Segment or Transmission Allocation	*Transmission Service Provider, Scheduling Entities (Intermediate Bas), Transmission Customer*
Any allowable correction to a Physical Load Segment	*Sink BA, Load Serving Entity*
Any allowable correction to a Market	*Purchasing-Selling Entity*

Segment	
Any allowable correction to any product code (energy or transmission) made by the e-Tag Author	*In addition to the above, the last Physical Transmission Segment's TSP, LSE, Sink BA*
TSP correction	*No re-evaluation required, no approval required*

Corrections are not permitted to add or remove participants from an e-Tag.

Approval Rights over the transaction remain as established in NERC/NAESB Standards. Entities impacted by corrections that are required to approve the transaction must be alerted to the correction. Upon receipt of a corrections submittal, the Authority resets the ActOnByTime and the TimeClassification based on the NERC/NAESB Interchange Standard Timing Tables.

NERC/NAESB Standards contain additional information regarding the processing of corrections.

1.6.2.3 Distributing a Profile Change Request

Profile Change Requests are distributed to all entities that received the original e-Tag. Depending on the type of change requested, the parties required to approve the Request may vary. NERC/NAESB Standards describe the entities required to evaluate the modification and the criteria they should use in their evaluation.

1.6.3 E-Tag Request Actions

1.6.3.1 Approving and Denying Requests

Approval entities will use a variety of methods, consistent with NERC/NAESB Standards, to determine whether an e-Tag Request should be approved or denied. Approval entities must actively approve or deny all requests within a specified Request evaluation period.

NERC/NAESB Standards provide details on the timing requirements under which requests should be made and evaluated.

When an approval entity decides to approve or deny a Request, the entity utilizes its Approval action to change the Approval State to "APPROVED" or "DENIED".

An approval entity has the option to change its Approval State at will, until the Request State has reached a final state.

If the entity wishes to indicate that it is reviewing a Request, but will not have an answer for some time, the entity can elect to change its Approval State to "STUDY". The action of placing an e-Tag in a "STUDY" state does not extend the approval window. The Approval Entity must still act in a timely manner to set the Approval State to "APPROVED" or "DENIED" before the Request evaluation deadline has passed.

The Authority collects these approval States and uses the indicated dispositions to determine transaction request implementation and rejection. NERC/NAESB Standards describe the manner in which an Authority determines the resolution of a particular pending Request. Once an e-Tag has reached a final state, all parties are informed of the resolution

1.6.3.2 Withdrawing a Request

For both New e-Tag Requests and Profile Change Requests, the Request initiator may withdraw the Request at any time up until the Request has reached a final state by submitting a WithdrawRequest message. If a Request has already been APPROVED, then that Request cannot be WITHDRAWN. In order to withdraw a Request, the initiator uses its Agent to send a request to the Authority to withdraw the Request. Upon timely receipt of the WITHDRAW request, the Authority will consider the Request WITHDRAWN and process that event accordingly, distributing notification of the Request State change to all parties.

The only party that may withdraw a Request is the original initiator of a Request or holder of the initiator's Security Key. No Request may be withdrawn without a valid Security Key.

1.6.3.3 Canceling a Request

Should an e-Tag's author wish to back out of a CONFIRMED e-Tag, that entity must submit a RequestTerminateTag message to the Authority. NERC/NAESB Standards describe the approval rights and responsibilities of the various entities involved in the approval process. If the cancellation request is approved, the Composite State of the e-Tag is set to CANCELLED and processed accordingly with both the energy and transmission allocation profiles set to zero.

1.6.3.4 Terminating an e-Tag

Should an e-Tag's author wish to back out of an IMPLEMENTED e-Tag, that entity must submit a RequestTerminateTag message that includes a valid termination time. NERC/NAESB Standards describe the approval rights and responsibilities of the various entities involved in the approval process. If the termination request is approved, the Composite State of the e-Tag is set to TERMINATED and processed accordingly. The energy and transmission allocation profiles will be set to zero effective at the specified start time.

Should an entity wish to correct an invalid ATF e-Tag, that entity must submit a RequestTerminateTag. NERC/NAESB Standards describe the approval rights and responsibilities of the various entities involved in the approval process. If approved, the Composite State of the e-Tag is set to TERMINATED and processed accordingly with both the energy and transmission allocation profiles being set to zero.

1.6.4 Information Distribution

1.6.4.1 Distribution of Request Approval State

When a significant status change occurs (as defined in section 3.6.4.1), the Authority responsible for the e-Tag will notify all parties of that change. By doing so all parties are advised of the current disposition of the e-Tag. In the case of entities electing to deny a New e-Tag Request, the e-Tag Author may attempt to correct the e-Tag in order to satisfy the needs of the denying party.

1.6.4.2 Distribution of Request Resolution

When the final disposition of a Request has been determined (e.g., APPROVED, DENIED, WITHDRAWN, etc.), the Authority responsible for the e-Tag will notify all parties electronically of the request's resolution. By doing so, all parties are advised that they should either implement or discard the request.

1.6.4.3 Distribution of Potential TLR Profile Change

Warning notifications of Potential TLR Profile Change are distributed electronically to each Purchasing-Selling Entity listed on the e-Tag. These notices are preliminary, and may not reflect final curtailments.

Warnings of Potential TLR Profile Change are issued at the time a Reliability Coordinator requests a set of curtailments, but prior to the final confirmation and issuing of those curtailments by the RAS. These warnings can be used by market participants to prepare for curtailments. The warnings may also be used by market participants to proactively modify their transactions in ways that address the reliability needs of the system without compromising the financial positions of the marketplace.

1.6.5 Query Functions

Queries may not be abused though excessive querying. General rules for this functionality are as follows:

- No service may query for the same data more than once (1) per minute
- Querying may NOT be considered a replacement for the requirement to have a dedicated listener for inbound information distributions. Services that observe behavior counter to these requirements may ignore such requests if the processing of those requests represents a threat to the integrity of the system. Prior to ignoring the requests, contact must be made with the offending entity and resolution be attempted. If the attempts to resolve the issue fail, the recipient of the requests may block those requests, provided.
    - The processing of those requests represents a real, *documentable* threat to the integrity of the system,

- The threat is fully documented (i.e., processor logs, customer complaints, etc…)
- That recipient has met the above minimum requirement, and
- The attempt to address the problem has been documented as well (i.e., E-Mails, Telephone recordings, etc…).

Some queries are processed through two-part messages, or asynchronous messages. In these types of messages, a query is made, and the recipient acknowledges receipt of the query, but does not respond immediately. The connection between the systems is broken, and the recipient processes the message. Upon completion of the processing, the recipient issues a callback message to the original query author and provides the results of the processing. In this manner, the recipient of the query may manage the processing of such queries more efficiently without threat to the integrity of the system (due to long complex queries that may take significant time and resources to process).

1.6.5.1 Querying for e-Tag Summaries

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query e-Tag Authorities for a list of e-Tag Summaries for a specified period of time for e-Tags in which they participate. Query parameters allow the ability to Retrieve e-Tag Summaries that:

- were created/last modified during a specified period of time, OR
- have a profile with the first start/last stop intersecting the specified period of time.

E-Tag data may be retrieved for past, current, or future time ranges. This method is intended to be used for emergency operational e-Tag recovery, and is not designed to be used for continuous real-time polling. The duration of the specified time period must not be greater than 24 hours. Entities can only retrieve e-Tag information through a listener registered for the entity they represent. Querying for e-Tag Summaries is an Asynchronous message.

1.6.5.2 Querying for an e-Tag

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query for the current data set that describes an e-Tag from the Authority. This includes all Request data associated with an e-Tag, including a new tag request. Entities can only retrieve e-Tag information for which they have presented valid security keys.

1.6.5.3 Querying for e-Tags

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query for a set of data that describes several e-Tags from the Authority. This includes all Request data associated with an e-Tag, including a new tag request. Entities can only retrieve e-Tag information for which they have presented valid security keys (or, for Asynchronous message, must have a listener registered for the entity they represent). Queries for multiple e-Tags are processed through Asynchronous messages.

1.6.5.4 Querying for an e-Tag's History

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query the Authority for a list of all of the methods that have been applied to a single e-Tag. This query allows a participant to re-construct the complete set of actions that were taken against an e-Tag. Entities can only retrieve e-Tag information through a listener registered for the entity they represent. Queries for multiple e-Tags are processed through Asynchronous messages.

1.6.5.5 Querying for Request IDs

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query an Authority for a list of Request IDs, in order to verify synchronization with the Authority's log of requests. Should an entity discover that they are not synchronized with the Authority then, this listing of Request IDs may be used to query an Authority node for the corresponding Request messages. The default behavior of the Authority node is to return all Requests grouped by Request State (e.g., PENDING, APPROVED, etc.) and ordered by original send time. An entity may ask that the listing be filtered based on one or more Request States. Once the Request ID listing has been retrieved, an entity may query the Authority node and retrieve sets of Request messages.
A Request ID listing may be used in two ways. The first is to notify an entity of requests they need to retrieve after communication failure. The second is for an entity to determine for itself which requests it needs after missing requests are detected. In either case, the Authority node may determine based on network traffic and the absence of messaging faults the number of Requests that may be retrieved at one time.
Entities can only retrieve e-Tag information for which they have presented valid security keys.

1.6.5.6 Querying for a Specific Request

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query the Authority for a copy of a specified Request. This query allows a participant to recover from missed requests against an e-Tag due to network or system failure. Entities can only retrieve e-Tag information for which they have presented valid security keys.

1.6.5.7 Querying for a Specific Request's State

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may query the Authority for the States of a specified Request. This query allows a participant to recover from missed requests against an e-Tag due to network or system failure. Entities can only retrieve e-Tag information for which they have presented valid security keys.

1.6.5.8 Querying for Service Availability

Any registered entity (PSEs, BAs, TSPs, Reliability Coordinators, etc.) may use the QueryAvailability message to query any e-Tagging service regarding its availability to process messages. For purposes of enforcing the restriction that "no service may query for the same data more than once (1) per minute", QueryAvailability messages sent to the same URL are considering to be querying for the same data, even if the ToEntity code is different in the messages.

Section 2 - Tag Agent Functional Requirements

2.1 Introduction

All Purchasing-Selling Entities (PSEs) and any other parties responsible for submitting Arranged Interchange shall communicate the necessary information via the Agent. The Agent shall comply with all functional requirements set forth in this document. Users may elect to comply with these Agent requirements using internally developed hardware/software, third party developed hardware/software, or third party subscription type services.

The Agent shall provide facilities to:

- Accept and validate input e-Tag data from the user.
- Generate all XML necessary to completely specify the transaction as defined in the e-Tag Data Model based on user input data.
- Assign and maintain the correspondence between each transaction's e-Tag ID and e-Tag Author's Security Key.
- Identify the Authority associated with the registered Sink Balancing Authority in the transaction and electronically communicate the e-Tag ID, Security Key, and associated e-Tag data to that Authority.
- Receive unsolicited information messages regarding e-Tags that they are a party to but for which they have no direct approval rights.
- Query Authorities for the current State of each transaction submitted by the user (or transaction to which the user has both e-Tag ID and e-Tag Author's Security Key).
- Provide the means for the user to correct any pending transaction submitted by the user (or transaction to which the user has both e-Tag ID and e-Tag Author's Security Key).
- Provide the means for the user to withdraw any pending transaction or request submitted by the user (or transaction to which the user has both e-Tag ID and e-Tag Author's Security Key).
- Provide the means for the user to modify any existing transaction submitted by the user (or transaction to which the user has both e-Tag ID and e-Tag Author's Security Key).
- Receive unsolicited information from the other e-Tag services regarding e-Tag updates, curtailment warnings, etc.

Information systems designed to provide more than one e-Tagging service (e.g., Agent and Authorities) are free to use any internal or proprietary mechanisms to convey e-Tag information between those functional services, but must still comply with all technical standards and protocols related to the exchange of transaction information with e-Tagging services provided by (or for) others.

2.2 Registry Usage

The Agent shall be responsible for maintaining an updated list of all registered entities whose identities must be uniquely specified in connection with the arrangement of an Interchange Transaction. The Electric Industry Registry of all such entities shall be maintained and available for downloading from the Electric Industry Registry web site. The Agent shall supply a procedure to allow updates from the Electric Industry Registry on demand as well as on a prescheduled interval. The Electric Industry Registry shall be in a format defined in a document posted on the Electric Industry Registry vendor's web site.
The Agent must support the receipt of unsolicited messages sent by Authorities. To enable the delivery of these messages, the user must register the appropriate service identification information in the Electric Industry Registry and be capable of receiving e-Tag messages.

2.3 Tag Data Entry and Viewing

The Agent shall provide a mechanism for the user to input, edit, and view e-Tags, as well as perform all other functional requirements described herein. The exact nature of this user interface is beyond the scope of this document, with the exception that the user shall have the facilities to supply all transaction related information necessary to create complete, valid e-Tags, as well as the interfaces to view those e-Tags.

2.3.1 Tag ID Creation

Each e-Tag submitted for approval to any Authority by the Agent shall be identified by an e-Tag ID. This e-Tag ID must not be identical to any used previously to represent transactions with effective stop dates less than one year in the past. *See Section 1.4.2.1 "Tag IDs"*.

2.3.2 Security Key Creation

A unique Security Key shall be associated with the initial transmission of an e-Tag from the Agent to the appropriate Authority. The Agent shall be responsible for generating this Security Key consisting of a unique 12 character token. All subsequent messages exchanged between the Agent and Authority in regard to this e-Tag shall refer to both the e-Tag ID and Security Key assigned by the user's Agent. *See Section 1.4.2.2 "Security Keys"*.

2.4 Date and Time Handling

The Agent shall be responsible for the conversion of all date and time related input fields to Universal Coordinated Time (UTC) prior to information being exchange with any other service. Valid times during the day shall be from 00:00:00 to 23:59:59. TheAgent user interface is free to accept and manage the conversion of any appropriate date/time formats at the discretion of the service provider. The internal representation of date and time within the Agent is also entirely at the discretion of the service provider. However, all electronic transmittal of data shall be in UTC time. E-Tag start and stop times must be on a minute boundary.

2.5 Data Validation

The Agent shall ensure that all data elements in a communication are legitimate and that no syntax or validation rules have been broken.

2.6 Function Implementation

The Agent is responsible for being able to call the following methods:

- RequestNewTag
- RequestCorrection
- RequestProfileChange
- WithdrawRequest
- RequestTerminateTag
- QuerySummaries
- QueryTag
- QueryTags
- QueryHistory
- QueryRequestIDs
- QueryRequest
- QueryStatus
- QueryAvailability

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeProfileChange
- DistributeStatus
- DistributeResolution
- DistributePotentialTLRProfileChange
- CallbackSummaries
- CallbackTags
- CallbackHistory
- QueryAvailability

Semantics, including calling and processing rules are described in detail in the following sections.

2.6.1 Initiating a Request

The following procedure should be used to validate and process a new e-Tag Creation request:

- Write the new request and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.

- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.

2.6.1.1 Submitting a New e-Tag Request

Write Request – The e-Tag Author must write a complete representation of the transaction being e-Tagged, as defined in NERC/NAESB Standards and the Data Model. The Author must also provide any additional parameters necessary to successfully call the RequestNewTag method. The Agent may elect to automate the provision of some of these parameters (i.e., Security Key, e-Tag Code, etc…). A new e-Tag Request must specify a proper Base Profile, as described in section 6.1.4.2.1. Specifically, Agents must submit all appropriate profiles, but are not allowed to submit Current Level profiles. All Correction IDs must be set to zero in the new e-Tag Request.

Verify Semantics – the following rules must be met in order to constitute a valid Request:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag being sent must not contain a Profile representing a transaction starting more than 168 hours in the past.
- ATF e-Tags must be no longer than one hour in duration.
- Should the Request not be valid, the e-Tag Author must be informed of the error(s) by the Agent and provided with an opportunity to rectify the violation.
- All applicable validations required in NERC INT-007-1 must be performed.
- The transmission allocation for all transmission segments must be greater than or equal to the minimum of the POR profile and POD profile for that segment.
- The earliest energy profile start time must be less than or equal to the earliest start time of any other profile type and the latest energy profile end time must be greater than or equal to the latest end time of any other profile type.
- If the Scheduling Entity field is left blank, the Agent must ensure that a BA tag code that is identical to the TSP tag code exists prior to submission to the Authority. If no BA tag code identical to the TSP tag code is found, the Request is invalid.

Store Reference Number – The Authority will assign the new e-Tag a reference number, through which the e-Tag Author may query for State. All new e-Tag requests will receive a request ID of zero (0).

2.6.1.2 Submitting a Correction Request

Write Request – The e-Tag Author is responsible for creating the e-Tag correction(s) if needed. The e-Tag Author must also provide any additional parameters necessary to successfully call the RequestCorrection method. The Agent may elect to automate the provision of some of these parameters (i.e., Security Key, e-Tag Code, etc…). When submitting a correction, the correction must contain all the necessary data to replace the existing data. For example, a correction to an OASIS number must not only contain the

OASIS number, but also the Transmission Allocation ID, a reference to the Parent Segment, the Product, and the associated Transmission Customer.

Verify Semantics – the following rules must be met in order to constitute a valid Request:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Corrections may not be made to e-Tags that have reached a final state (e.g., IMPLEMENTED, etc.)
- Corrections may not be made that violate the rules defined in NERC/NAESB Standards regarding appropriate use of correction

Should the Request not be valid, the e-Tag Author must be informed of the error(s) by the Agent and provided with an opportunity to rectify the violation.

Store Reference Number – The Authority will assign each correction a number that is used to indicate the most recent correction to be applied to a specific segment or allocation (or set of such changes). The Agent must record these numbers for later reference and integrity verification.

2.6.1.3 Submitting a Profile Change Request

Write Request – The e-Tag Author must write a complete representation of the Profile Change to the e-Tag. The Author must also provide any additional parameters necessary to successfully call the RequestProfileChange method. The Agent may elect to automate the provision of some of these parameters (i.e., Security Key, e-Tag Code, etc…). e-Tag Authors are required to submit all necessary profiles to support the desired change(s); Authorities will not auto-generate upstream/downstream values as done during reliability limit setting. Agents are not allowed to make changes to the Reliability limits. Furthermore, Agents are not allowed to submit Current Level profiles, because these profiles are calculated.

Verify Semantics – the following rules must be met in order to constitute a valid Request:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Profile Changes can only occur once an e-Tag has transitioned to the Composite State of CONFIRMED OR IMPLEMENTED.
- Profile Changes must not affect points in time more than one (1) hour in the past with the exception of DYNAMIC e-Tags which must not affect points in time more than 168 hours in the past.
- Extensions must be received NO LATER than the last time specified in any profile in the e-Tag. E e-Tags may NOT be extended once the e-Tag's profile (including any previous extensions) has been completed. ATF e-Tags may not be extended.

Should the Request not be valid, the e-Tag Author must be informed of the error(s) by the Agent and provided with an opportunity to rectify the violation.

Store Reference Number – The Authority will assign the Profile Change a request number through which the e-Tag Author may query for Request State. That number will always be greater than zero (0).

Additional Function Implementation Details
It is possible for an e-Tag Author to supply changes to the transmission allocation when specifying a profile change. The following rules should be noted:

- It is impossible to delete a transmission allocation. If a reservation needs to be eliminated, its profile must be adjusted to zero.
- A new transmission allocation may be added at any time. This addition will result in the creation of a new reservation allocation and new Base Profile. The transmission allocation will NOT be added as an Exception Allocation since a previous Base Profile does not exist. (See section 6.2.5 for more information on Allocation Profiles.). Transmission allocation IDs must not be re-used, regardless of Request State.
- Should an e-Tag Author need to modify a transmission allocation then the e-Tag Author must specify the change in the same manner in which profile change or extension would be performed. For example, if a request was made to extend an e-Tag for an additional hour (while intending to utilize the same transmission reservation as used in the previous hour), then an allocation exception would be inserted that specified the additional hour.

Modifications to DYNAMIC type e-Tags more than one hour in the past are used to set the actual interchange quantity. The current level needs to be set to this actual interchange quantity regardless of any other profile values. This is achieved by clearing any existing reliability limit and setting the Market Level profile.

2.6.2 Request Distribution

The Agent only receives three types of Request Distribution – New e-Tag Request Distributions, Correction Request Distributions, and Profile Change Request Distributions.
Upon receiving a distribution message, the agent software should decode, parse, and validate the XML message. If the message doesn't pass syntactic and semantic validation, then the agent must return a fault or error response to the sender. If the message does pass validation, then the agent must return a success response to the sender. Either way, the Agent software is required to provide a valid XML response (success or failure) to the sender of any distribution message.

2.6.2.1 Processing a New e-Tag Request Distribution

New e-Tag Request Distribution messages must pass the following rules in order to be considered valid:

- The rules described in the Data Model and Method sections must not be violated
- An e-Tag with the ID presented must not already exist on the Agent

2.6.2.2 Processing a Correction Request Distribution

Correction Request Distribution messages must pass the following rules in order to be considered valid:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Corrections may not be made to e-Tags that have reached their final state (e.g., IMPLEMENTED, etc.)
- Corrections may not be made that violate the rules defined in NERC/NAESB Standards regarding appropriate use of correction

Upon receipt of a valid Correction Request Distribution, the Agent must take the following actions:

- Immediately replace the previously received information with the corrected information
- Alert the Agent Operator that the correction has occurred, highlighting the correction for their inspection
- Immediately consider re-setting any previous e-Tag assessment action (APPROVED, DENIED, STUDY, etc.) of an approval entity that is impacted by the correction

2.6.2.3 Processing a Profile Change Request Distribution

New Profile Change Request Distribution messages must pass the following rules in order to be considered valid:

- The e-Tag ID Referenced in the message must be one held by the Agent
- The rules described in the Data Model and Method Descriptions sections must not be violated

2.6.3 Request Actions

2.6.3.1 Approving and Denying Requests

The Agent has no requirements with regard to Request Approval and Denial.

2.6.3.2 Withdrawing a Request

The following procedure should be used to withdraw a Request:

- Write the withdraw message and encode it in a valid XML format (as described by the latest e-Tag schema). The Message must include the following items:
    - The Request ID provided by the Authority at the time the request was made.
    - The original Security Key for the transaction that was used in the e-Tag Creation message.
    - A reason that explains why the Withdrawal was made.

- Withdraw messages must not be sent for requests that have already reached a final state (IMPLEMENTED, DEAD, etc.).
- Withdraw messages may be sent for ATF Requests that have a Request State of PENDING.
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- The Request State is set to WITHDRAWN.
- WITHDRAWN is a final state.

2.6.3.3 Cancelling an e-Tag

The following procedure should be used to cancel an e-Tag:

- Write the RequestTerminateTag message and encode it in a valid XML format (as described by the latest e-Tag schema). The message must include the original Security Key for the transaction that was used in the e-Tag Creation message. Specify the termination time as the block start time of the e-Tag.
- RequestTerminateTag messages must only be sent for e-Tags with a Composite State of CONFIRMED, IMPLEMENTED, or TERMINATED.
- The RequestTerminateTag message must contain a termination start time that is equal to the block start time (if it is later it could only transition to TERMINATED).
- Only CONFIRMED e-Tags may transition to CANCELLED e-Tags.
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- Upon cancellation, all pending requests for the cancelled e-Tag are set to a Request State of DENIED.
- CANCELLED is a final Composite State.

2.6.3.4 Terminating an e-Tag

The following procedure should be used to cancel or terminate an e-Tag:

- Write the RequestTerminateTag message and encode it in a valid XML format (as described by the latest e-Tag schema). The Message must include the Request ID

provide by the Authority at the time the request was made and the desired termination time. The termination message must also include the original Security Key for the transaction that was used in the e-Tag Creation message.

- RequestTerminateTag messages are only valid for requests that have reached the state of CONFIRMED, IMPLEMENTED, or TERMINATED.
- RequestTerminateTag messages may be used for IMPLEMENTED ATF e-Tags.
- Termination of a TERMINATED e-Tag may only change the termination time to an earlier time than the last approved RequestTerminateTag Request.
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- Once approved, the Composite State of the e-Tag becomes CANCELLED or TERMINATED.
- Both CANCELLED and TERMINATED are final states.
- It is acceptable to terminate an e-Tag multiple times, assuming that the termination time of each termination message is earlier than the termination time of the prior termination messages.
- Upon the RequestTerminateTag request becoming APPROVED, all PENDING RequestProfileChange requests with block end time after the termination time, and all PENDING RequestTerminateTag requests with termination time after the APPROVED Request's termination time, are set to a Request State of DENIED.

2.6.4 Information Distribution

2.6.4.1 Processing a Request Approval State Distribution

The following validation criteria must be checked when an Agent receives a Request Approval State Distribution message:

- The e-Tag ID Referenced in the message must be one held by the Agent
- The Security Key presented must be identical to the original Security Key provided at the time the Agent transferred the New e-Tag Request to the Authority
- The rules described in the Data Model and Method Descriptions sections must not be violated

2.6.4.2 Processing a Request Resolution Distribution

The following validation criteria must be checked when an Agent receives a Request Resolution Distribution message:

- The e-Tag ID Referenced in the message must be one held by the Agent

- The Security Key presented must be identical to the original Security Key provided at the time the Agent transferred the New e-Tag Request to the Authority
- The rules described in the Data Model and Method Descriptions sections must not be violated

When a Request is resolved to a state of APPROVED, then it should be considered complete and the Request data should be applied to the e-Tag. When a Request is resolved to WITHDRAWN, DENIED, or EXPIRED the data in the Request should be disregarded.

2.6.4.3 Processing a Potential TLR Profile Change Distribution

The following validation criteria must be checked when an Agent receives a Potential TLR Profile Change Distribution message:

- The e-Tag IDs Referenced in the message must be held by the Agent
- The rules described in the Data Model and Method Descriptions sections must not be violated

Agents may elect to verify the validity of the Potential TLR Profile Change Distribution. To do this, the Agent must send a Callback message to the RAS that issued the Potential TLR Profile Change Distribution. The Callback must contain the same security key presented to the Agent as part of the original TLR Profile Change Distribution message. If the Agent is unable to connect to the RAS or if the RAS replies with a Fault, the Agent should attempt to retry the message, as described in section 7.1.1.1.

2.6.5 Query Functions

2.6.5.1 Synchronous Queries

Synchronous Queries include the following:

- Query e-Tag
- Query RequestIDs
- Query Request
- Query State
- Query Availability

The following procedure should be used to initiate all synchronous queries:

- Write the query and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP POST message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before

attempting resubmission. If the response succeeds, then process any data returned by the Authority.

2.6.5.1.1 Query for an e-Tag

Agent must specify a valid e-Tag ID and the associated Security Key they used to submit the original New e-Tag Request.

2.6.5.1.2 Query for Request IDs

Agent must specify a valid e-Tag ID and the associated Security Key when submitting the original New e-Tag Request. Optionally, the user may elect to filter Request ID's based on the resolution of the requests associated with the e-Tag (i.e., show only IMPLEMENTED Requests).

2.6.5.1.3 Query for a Request

Agent must specify a valid e-Tag ID and the associated Security Key when submitting the original New e-Tag Request, as well as the Request ID they wish to retrieve.

2.6.5.1.4 Query for a Request's State

Agent must specify a valid e-Tag ID and the associated Security Key when submitting the original New e-Tag Request, as well as the Request ID for the desired State information.

2.6.5.1.5 Querying for System Availability

Agent must specify a particular system for which to query availability - by both entity desk and e-Tag service (Agent, Approval, Authority, or RAS).

Agents should respond back to Queries for System Availability as follows:

- If the Agent is operating correctly, the Return Value should be SUCCESS.
- If the Agent is not operating correctly, the Return Value should be FAIL.
- If a known error is occurring, the Agent should indicate that error.

2.6.5.2 Asynchronous Queries

Asynchronous Queries include the following:

- Query Summaries
- Query e-Tags
- Query History

The following procedure should be used to initiate all asynchronous queries:

- Write the query and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP POST message, and wait for the response.

- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- Wait for a response message from the Authority. The response message will be over a new HTTP connection (not part of the query submission described in previous steps). The response will be sent to the Agent's registered service URL, and will include the same security key used by the Agent to submit the query. The Agent should perform syntactic and semantic validation on the query response message from the Authority, and reply to the query response message with either a success reply or a Fault/Error reply.

2.6.5.2.1 Query Summaries

Agent must specify either an Active Range or a Last Modified Range for which the e-Tag summaries should be returned. The Active Range is used to specify a range of time during which an e-Tag must have been "active" (i.e., start or end date/time of the e-Tag falls within the Active Range). The Last Modified Range is used to specify a range of time during which the e-Tag had a Request made against it (New e-Tag Requests, Correction Requests, and Profile Change Requests).

When an approval or agent service requests recovery over an outage range, the service must create a list of unique URL's for Authority services and send the Query Summary messages to each authority service in order to retrieve all e-Tags for which that e-Tag approval or agent service is a party. For Authorities that are shared between multiple companies, only one QuerySummaries message is required. The Tag Authority should return data for all tags that are visible to the requestor in this case, regardless of which the Authority's companies is listed as the intended message recipient.

Agent must also generate and specify a Security Key with which the Callback can be secured.

The following validation criteria must be checked when an Agent creates a Query Summaries message:

- The rules described in the Data Model and Method Descriptions section must not be violated
- The Range specified must not exceed twenty-four (24) hours. Authorities are only required to provide 24-hours of information in response to any single query.

The following validation criteria must be checked when an Agent receives a Query Summaries Callback message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The Security Key presented must be identical to the original Security Key provided at the time the Agent transferred the Summaries Query to the Authority

2.6.5.2.2 Query e-Tags

The Agent service must provide a list of e-Tag IDs and Security Keys for all e-Tags to be queried. The Agent must also specify a Return Rate, which indicates how many e-Tags the Agent wishes to receive within each callback. Missing security keys can be recovered using the Query Summaries message. The User must also specify a separate Security Key for the query with which the Callback can be secured.

Special Note: Query e-Tags may return more than one callback, depending on how the user configures their original query and how the Authority is configured.

The following validation criteria must be checked when an Agent receives a Query e-Tags Callback message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag IDs presented must match the e-Tag IDs requested in the original query
- The Security Key presented must be identical to the original Security Key provided with the original query

2.6.5.2.3 Query History

Agent must specify a valid e-Tag ID and Security Key. The security key should be the same key that was used when creating the e-Tag (for e-Tag authors), or the security key provided by the Authority through a Distribute message. Missing security keys can be recovered using the Query Summaries message.

The following validation criteria must be checked when an Agent receives a Query History Callback message:

- The e-Tag ID presented must match the e-Tag ID requested in the original query
- The Security Key presented must be identical to the original Security Key provided with the original query
- The rules described in the Data Model and Method Descriptions sections must not be violated

2.7 Availability and Performance

Availability and performance requirements are specified in NERC/NAESB Standards, as well as a description of what actions to take during a system outage to ensure transaction of business is not halted.

Section 3 - Tag Authority Functional Requirements

3.1 Introduction

All entities responsible for performing the Balancing Authority (BA) function shall provide the necessary hardware, software, and/or services to implement the Authority. The Authority shall comply with all functional requirements set forth in this section. BAs may elect to comply with these Authority requirements using internally developed hardware/software, third party developed hardware/software, or third party subscription type services.

The Authority shall provide facilities to:

- Accept as input e-Tag data transferred in compliance with this document from any Agent.
- Provide immediate syntactical validation of the incoming data stream and respond accordingly.
- Identify all entities having approval rights over the transaction request, and transfer the request to the associated Approvals for evaluation
- Identify all entities entitled to an informational copy of the transaction request, and transfer the request to the associated Agents and Approvals.
- Manage each request's approver's Approval States and overall Request State based on communication with the Agent and Approvals.
- Verify the identity of each approval entity attempting to approve or deny a Request based on the presented e-Tag ID and Security Key, and update the entity's Approval State and the Request State, as appropriate.
- Provide facilities for overriding Approval States on the behalf of an Approving entity.
- Verify the identity of each requesting entity attempting to make a request based on the presented e-Tag ID and Security Key, and create the Request as appropriate.
- Generate notification messages to Approvals and Agents as appropriate.
- Respond to inquiries for transaction information made by Agents or Approvals.
- Store all e-Tags, to be available for on-line querying and access, for at least ninety (90) days after the stop date/time in the e-Tag.

Information systems designed to provide more than one e-Tagging service (e.g., Authority and Approvals) are free to use any internal or proprietary mechanisms to convey e-Tag information between those functional services, but must still comply with all technical standards and protocols related to the exchange of transaction information with e-Tagging services provided by (or for) others.

3.2 Registry Usage

The Authority shall be responsible for maintaining an updated list of all registered entities whose identities must be uniquely specified in connection with the arrangement of an Interchange Transaction. The Electric Industry Registry of all such entities shall be maintained and available for downloading from the Electric Industry Registry web site. The Authority shall supply a procedure to allow updates from the Electric Industry Registry on demand or on a prescheduled interval. The Electric Industry Registry shall be

in a format defined in a document posted on the Electric Industry Registry vendor's web site.

Each BA shall provide the necessary information to identify in the Electric Industry Registry who serves as their Authority when that particular BA is referenced as the Sink BA in an e-Tag.

3.3 Tag Data Entry and Viewing

The Authority is primarily an automated manager of data that should require little manual intervention. However, certain events may require user interaction. To this end, The Authority shall provide a mechanism for a user to view e-Tag requests and **directly modify/override entity Approval States**, as well as perform all other functional requirements described herein. The exact nature of this user interface is beyond the scope of this document; with the exception that the user shall have the facilities to view all information (as described in this document) contained in a valid e-Tag.

3.3.1 Approval State Override

As required above, Approval States may be overridden by the Authority operator. Such overrides must occur within the normal bounds of the state management logic:

- Approval States cannot be overridden for requests that have already reached a final state (i.e., IMPLEMENT, CANCELLED, etc.)
- Overrides must be treated exactly the same as if the approver had set the Approval State (i.e., if a state setting would normally move the Request to a state of IMPLEMENT, then an override to the same state must have the same result).

The ability to override Approval States must only be utilized in the event that the entity whose state is being overridden has requested the Authority operator to do so due to communication or system failure.

3.3.2 Security Keys

The Authority shall be responsible for managing Security Keys associated with e-Tag requests. Security Keys for Agents are chosen by the Agent itself; all other Security Keys (with the exception of the IDC Security Key described below) are assigned and managed by the Authority.
Each Authority shall be assigned a unique IDC Security Key to be used when communicating with the IDC. All communications with the IDC must use this IDC Security Key in order to be considered valid. The IDC will reject any messages without a valid IDC Security Key. The IDC e-Tag Key must be considered confidential.

3.4 Date and Time Handling

The Authority shall be responsible for the conversion of all date and time related input fields to Universal Coordinated Time (UTC) prior to information being exchanged with any other service. Valid times during the day shall be from 00:00:00 to 23:59:59. E-Tag start and stop times must be on a minute boundary. The Authority user interface is free to

accept and manage the conversion of any appropriate date/time formats at the discretion of the service provider. The internal representation of date and time within the Authority is also entirely at the discretion of the service provider. However, all electronic transmittal of data shall be in UTC time.

The Authority Service must calculate the latest approval time in order to determine when to end the approval period and set the final Request State of an e-Tag. The absolute date/time by which an e-Tag may be approved is calculated based on a combination of the NERC/NAESB timing guidelines and the application of the start ramp duration defined in the first profile block in the e-Tag and e-Tag start time. If the first energy profile block in the e-Tag does not contain a ramp duration or if the first energy profile block does not start at the e-Tag start time, then default ramp durations should be used. Default ramp durations are defined in NAESB Standard R05001. The default ramp durations must be used in conjunction with the NERC/NAESB timing guidelines to determine the absolute time limit for approval in the absence of a ramp duration supplied by the e-Tag Author.

The ramp type for all interchanges between balancing authorities is a straddle ramp. Straddle ramps divide the start ramp duration equally across the profile block start time and divide the end ramp duration equally across the profile block end time. When the e-Tag contains multiple profile blocks, the ramp duration in the profile block's ramp start duration is used to calculate ramp start time and instantaneous MW levels. The ramp end duration is ignored in all profile blocks except for the last profile block where it is used to calculate the ramp end time and instantaneous MW levels. The ramp start time can be determined by dividing the ramp duration by two and subtracting it from the profile block start time. The start time derived from the first profile block is used to determine the point at which the e-Tag transitions from CONFIRMED to IMPLEMENTED. The ramp continues from the ramp start time across the profile block start time to the ramp duration minutes divided by 2 after the profile block start time.

The default ramp duration for reliability adjustments is ten minutes (for all interconnections). Ramp rates may be optionally supplied by the entity requesting the profile change. When a reliability adjustment is made, it may result in the creation of additional profile blocks. The ramp durations of the profile blocks will need to be adjusted in this case with the ramp start duration of the adjusted block being set to ten minutes or the supplied start ramp duration and the rest of the ramp start durations (and end duration in the final block if applicable) remaining with their associated profile blocks.

3.5 Data Validation

The Authority shall ensure that all data elements in a communication are legitimate and that no syntax or validation rules have been broken.

3.6 Function Implementation

The Authority is responsible for being able to call the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeProfileChange
- DistributeStatus
- DistributeResolution
- DistributeTerminateTag
- CallbackSummaries
- CallbackTags
- CallbackHistory

And process the following methods:

- RequestNewTag
- RequestCorrection
- RequestProfileChange
- SetState
- WithdrawRequest
- RequestTerminateTag
- QuerySummaries
- QueryTag
- QueryTags
- QueryHistory
- QueryRequestIDs
- QueryRequest
- QueryStatus
- Query Availability

Semantics, including calling and processing rules are described in detail in the following sections.

The Authority is also responsible for Request State Management, as described in section 1.3.4.2 and 1.3.4.3. Passive State settings due to time elapse are also the responsibility of the Authority.

3.6.1 Initiating a Request

3.6.1.1 Processing a New e-Tag Request Submission

The security key presented with the Request e-Tag message will be used by the Authority for all future messages from/to the e-Tag author for this e-Tag. Authority must compare the e-Tag's start time or calculated ramp start time to the NERC/NAESB Standards timing guidelines. The e-Tag is considered to be LATE, ATF or on time as per those guidelines. E-Tag start and stop times must be on a minute boundary. E-Tags submitted after the e-Tag stop time (as determined by the time of receipt at the Authority) must be considered to be ATF and designated as such. The corresponding enumeration must be

set by the Authority Service and must be persistent, reset only if e-Tag Author makes a correction.

The following validation criteria must be checked when an Authority receives a Request e-Tag message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- An e-Tag with the ID presented must not already exist on the Authority
- If a Transmission Segment's POR or POD is listed as a DC Tie facility, then the associated Balancing Authority for that DC Tie must be listed as a Scheduling Entity for that Transmission Service Provider.
- A New e-Tag Request may not create an e-Tag that starts more than 168 hours in the past.
- An ATF e-Tag must be no longer than one hour in duration.
- All applicable validations required in NERC INT-007-1 must be performed.
- The transmission allocation for all transmission segments must be greater than or equal to the minimum of the POR profile and POD profile for that segment.
- The earliest energy profile start time must be less than or equal to the earliest start time of any other profile type and the latest energy profile end time must be greater than or equal to the latest end time of any other profile type.
- If the Scheduling Entity field is missing, the Authority must ensure that a BA tag code that is identical to the TSP tag code exists. If no BA tag code identical to the TSP tag code is found, the Request is invalid.

Once an e-Tag Creation request passes validation, the Authority must store the e-Tag in its local data store and identify it as a Pending Request. In so doing, it must generate the appropriate "Current Level" profile. The initial Current Level profile must be stored by the Authority service if "In-Kind" losses are specified so it may later be used for loss accounting, replaced only when market level profile change requests are approved. For each supplied base profile, the *Current* base profiles will be generated. For all transactions and all profiles, the Current Level is equal to the specified Market Level.

The Current Level profile should not be distributed, but rather derived based on all approved Requests associated with a particular e-Tag, processed in order of receipt by the Authority.

Upon receipt, the Authority sets the ActOnByTime and the TimeClassification based on the time of receipt and the NERC/NAESB Interchange Standard timing tables.

The Authority must then build the distribution table for the e-Tag. Details follow in the section below. Once the distribution list has been determined, the Authority must distribute the e-Tag to the appropriate parties.

3.6.1.1.1 Identifying the Distribution List

Tag Authorities must determine the distribution list for an e-Tag. The distribution list is comprised of the following entities as listed on the e-Tag:

- The e-Tag Author
- The Generation Providing Entity (Merchant)
- The Load Serving Entity
- All Intermediate Purchasing Selling Entities (Title Holders)
- All Transmission Customers
- The Balancing Authority in which the generation is located (Source BA)
- The Balancing Authority in which the load is located (Sink BA)
- All Transmission Service Providers
- All Scheduling Entities for those Transmission Service Providers
- All Reliability Coordinators listed in the Electric Industry Registry as being associated with the Source BA, Sink BA, and intermediate BAs.
- All entities contained in the CC list.

In order to determine a Service URL for the above entities, the following rules must be used:

- For GPEs, LSEs, and Transmission Customers, there will be potentially two entries. The first Service URL will be the entity's registered URL for their Agent service. The second Service URL will be the entity's registered URL for their Approval service.
- For intermediate PSEs, the Service URL will be the entity's registered URL for their Agent service.
- For all other entities, the Service URL will be the entity's registered URL for their Approval Service.
- For the GPE, LSE, and Transmission Customer, approval rights may be held, delegated, or waived. When holding rights, the Service URL is based on the registered approval URL for that entity. When delegating rights, the Service URL is based on the approval URL of the alternate entity specified for the specific source/sink in the e-Tag; this delegation always supersedes that specified as the registered approval URL for the GPE/LSE/TC. If the delegated entity is not already in the distribution list, the entity must be added. When waiving rights, the entity will have explicitly not listed an approval service in their registration or that of the source/sink.
- Entities identified in the CC list must not be given approval rights though the e-Tag may be distributed to the entities registered URL for their Approval Service as described in section one of this document.

No duplicate entities may be in the distribution list. A duplicate is defined as entities sharing both the same entity type (BA, TSP, PSE, RC), NERC Acronym, Service Type (i.e., Agent, Approval, Authority), and Service URL. Any entity that does not have a registered Service URL shall be removed from the distribution list, and any approval rights waived. Each entity will have a record in the list, identifying their Delivery URL for the transaction. A record in the list should have the following general format:

TAG ID	REQUEST ID	ENTITY CODE	SERVICE TYPE	SERVICE URL

3.6.1.2 Processing a Correction Request Submission

The following validation criteria must be checked when an Authority receives a Request Correction message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The Security key presented must be identical to the key presented to the Authority at the time the e-Tag was originally submitted by the Agent.
- Only the e-Tag Author or TSP may issue a correction
- Corrections are only allowed for e-Tags that are in a PENDING state.
- Only certain items may be corrected on an e-Tag. Specifically, the following are NOT allowed:
    - Addition or removal of any entity from the transaction path (both financial and physical)
    - Changes to the Energy profile (changes to the transmission allocations are acceptable)
    - Reassignment of a Transmission Allocation to a new Parent
    - Addition or Removal of any Scheduling Entity
- TSP authored corrections may only change the TransProductRef and transmission allocation on a physical segment where they are the associated TSP. The total transmission allocation MWlevel may not be changed (increased or decreased) for any period. Extensions are prohibited.

Once a Correction Request passes validation, the Authority must recompute ActOnByTime and TimeClassification using the correction's submission time in place of the e-Tag submission time and following the rules from the NERC/NAESB Standards timing guidelines. For TSP authored Correction Requests, since no approval process is required, the Authority must assign the same values active for the e-Tag for the ActOnByTime and TimeClassification. The Authority must then assign an incremental unique number to the correction, and each item being corrected must be updated to reflect this number. The first correction must be considered correction ID one (1). The response must contain references to the versions of the corrected segments.
The Authority must REPLACE the data in its current store with the new correction data. Any entity impacted by the correction (as defined in Section 1.6.2) must have their Approval State reset to PENDING and be informed of the change through Correction Request Distribution.

3.6.1.3 Processing a Profile Change Request Submission

The following validation criteria must be checked when an Authority receives a Request Profile Change message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The Security Key presented must be identical to the key associated with the Profile Change requester. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, the key will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- Profile Change Requests are only allowed for e-Tags that have been CONFIRMED or IMPLEMENTED
- Profile Change Requests may only change hours that are at the EARLIEST one (1) hour in the past. Dynamic tags are an exception to this rule (they may be changed up to 168 hours in the past).
- Profile change requests may not be made to extend an e-Tag once the e-Tag's profile has been completed (i.e., current time is equal to or later than the last date/time specified in the e-Tag).
- Reliability Limits may be set and cleared for any duration.
- Only certain entities may change certain profile values.
- Reliability Limits may specify the applicable BaseProfileID. The default location of the limit is at the GCA (BaseProfileID 1).
- Profile change requests made by the e-Tag author will use the source profile for loss calculations and will replace the profile stored on the Authority for use in loss calculations once the Request has reached a CONFIRMED or IMPLEMENTED state.
- Reliability Limits may not be changed for DYNAMIC e-Tags more than one hour in the past (but may be cleared).
- All applicable validations required in NERC INT-007-1 must be performed.
- TSP Market Profile changes may only impact the TransProductRef and transmission allocation on a physical segment where they are the associated TSP.
- TSP Market Profile changes may not reduce or increase the total transmission allocation MWlevel for any period. Extension is prohibited.
- TSP Market Profile changes cannot impact any MWlevel or Product in the past. Changes are bound in time with the earliest possible change starting at the time the Authority receives the Request and the latest possible change ending at the Tag Stop Time.

Upon receipt, the Authority sets the ActOnByTime and TimeClassification based on the time of receipt and the NERC/NAESB Interchange Standard timing tables. TSP Market Profile changes to the Product Code or Transmission Allocation requires no approval process therefore ActOnByTime should be set to the time of receipt and TimeClassification should be set to "On Time".

If the Request changes the reliability limit, then the Authority must calculate the correct MW values to use for all profiles except for the source profile (which is included in the Profile Change message). The source profile will be associated with a physical location (BaseProfileID). If no physical location is included in the Profile Change message then the Authority will default the location to the GCA. The value of each profile calculated

below must use the location information to calculate the correct profile values for both upstream and downstream profiles. The value of the profile at the physical segment specified in the Profile Change message will be the same as the source profile. The process for calculating upstream and downstream profiles is done in three steps: Loss Percentage, Carry Forward, and the New Limit calculation. The first step is to calculate the Loss percentage supplied by the creator of the original e-Tag based on the current MARKET LEVEL. This is done by applying the specified formula, for the day the curtailment is effective.

$$LossPercentage = \frac{TotalDailyMWhPOR - TotalDailyMWhPOD}{TotalDailyMWhPOR}$$

To minimize overpayments or underpayments when calculating the POD Megawatt profile under a curtailment a CarryForward concept is used to ensure that the delivering party is not over-charged with losses for the transaction. The starting value of CarryForward will always be zero. Afterwards, the CarryForward value must be re-calculated each hour or part of an hour for which a new curtailment has been applied to the profile.

$$CarryForward_N = 0$$

$$NewLimit_N = SpecifiedLimit - RoundUP(SpecifiedLimit * LossPercentage)$$

After the first calculation of the NewLimit, a CarryForward will exist and should be calculated as:

$$CarryForward_{N+1} = RoundUP(SpecifiedLimit * LossPercentage) - (SpecifiedLimit * LossPercentage)$$

Afterwards, curtailment should use the CarryForward value to calculate the new limit as:

$$NewLimit_{N+1} = SpecifiedLimit - RoundUP(SpecifiedLimit * LossPercentage - CarryForward_{N+1})$$

Example:

Daily MWh POR = 100 MW
Daily MWh POD = 97 MW
SpecifiedLimit (Curtailed to) = 50 MW

$$LossPercentage = \left(\frac{100 - 97}{100}\right) = 0.03$$

$$CarryForward_{N0} = 0$$

$$NewLimit_{N0} = 50 - RoundUp(50 * 0.03) = 50 - 2 = 48$$

$CarryForward_{N+1} = RoundUp(50 * 0.03) - (50 * 0.03) = 2 - 1.5 = 0.5$

Second Curtailment occurs to 40 MW

$NewLimit_{N+1} = 40 - RoundUp(40 * 0.03 - 0.5) = 40 - RoundUp(.7) = 39$ If a Reliability Limit Clearing is applied, then reliability limits for all periods following the start of the Clearing through the end of the clearing are set to null and the limits erased.

Once the downstream reliability profiles have been created, the Authority must generate the appropriate "Current Level" exception profiles. The exception profiles must only reflect the hours changed, NOT the entire transaction. The current *exception* profile will always be generated based on the following rules:

For PSE-Originating Market Changes:

For each supplied Exception Profile

- The Exception Current Level is set to the lesser of the effective Reliability Limit for the profile and the Exception Market Level. Effective Reliability Limit is defined as the current Exception Reliability Limit if one exists; if none exists, then the Reliability Limit is assumed to be infinite.

For Source BA/TSP/Sink BA-Originating Reliability Changes:

For Generation Profiles:

- The Exception Current Level is set to the lesser of the effective Market Level for the profile and the specified Exception Reliability Limit. Effective Market Level is defined as the current Exception Market Level if one exists; if none exists, then the Market Level is assumed to be the originally specified Base Market Level.

For each POR, POD, and Load Profile:

- The Exception Current Level is set to the lesser of the effective Market Level for the profile and the previously calculated Exception Reliability Limit. Effective Market Level is defined as the current Exception Market Level if one exists; if none exists, then the Market Level is assumed to be the originally specified Base Market Level Exception

For any Exception Profile where the Current Level is equal to the Base Current Level, the Exception Profile must be eliminated. This is intended to reduce redundant data exchange.

Additional Implementation Details

It is possible for an e-Tag Author or TSP to supply changes to the transmission allocation when specifying a profile change. The following rules must be noted:

- It is impossible to delete a transmission allocation. If a reservation needs to be eliminated, its profile must be adjusted to zero.
- A new transmission allocation may be added at any time. In so doing, a new reservation allocation and new Base Profile will be added. The reservation allocation will NOT be added as an exception allocation, as no previous base exits to be modified.
- Should an e-Tag Author need to modify an allocation, the changes must be specified in the same manner in which profile change or extension would be processed. For example, if a request was made to have a transaction for an additional hour, and the requestor desired to use the same reservation that was used for the previous hour, an allocation exception would be inserted that specified the additional hour.
- TSPs may not submit a transmission allocation change that modifies the pre-existing transmission allocation MWlevel for any period. Extension is prohibited.
- TSP transmission allocation adjustments cannot impact any MWlevel or Product in the past. Changes are bound in time with the earliest possible change starting at the time the Authority receives the Request and the latest possible change ending at the Tag Stop Time.

Following this modification of the allocation the ChangeRequest is distributed to all appropriate parties.

3.6.2 Request Distribution

The following procedure should be used when sending Request Distribution messages:

- Encode the new Request in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the intended recipient of the distribution message
- If the submission fails or the response contains fault messages, attempt to resend the message using the process described in section 7.1.1.1.
- Set the delivery status to an appropriate value indicating whether or not the message was successfully delivered to the intended recipient. Appropriate values are DELIVERED (no errors), COMMFAIL (couldn't contact the message recipient) and INVALID (an error was returned by the message recipient)

Identifying the Entities with Approval Rights

Some of the entities in the Distribution List will have Approval Rights over the various requests, while others will have only viewing rights. The rules for determining who has Approval Rights to each Request are defined in Section 1.6.2.1 of this document.

The Authority will need to maintain a RequestApprovalRights list for each e-Tag. This list will be used in generating the appropriately formatted distribution messages for delivery to the various distribution entities. The list will also be used to store local State information about each entity. Each entity will have a record in the list, defining their Delivery State, Approval State, and State Type. Initial delivery state (before delivery has been attempted) should be set to PENDING. A record in the list should have the following general format:

TAG ID	REQUEST ID	ENTITY CODE	DELIVERY URL	DELIVERY STATE	APPROVAL STATE	STATE TYPE

Each Request requiring Approvals (New e-Tag Request, Profile Change Request) must have a data set of this type associated with it. Entities with Approval rights will have their Delivery State set to QUEUED, their Approval State set to PENDING, and their State Type set to NA.

Entities without Approval Rights will have their Delivery State set to QUEUED, their Approval State set to NA, and their State Type set to NA.

An entity authoring a Request will be assumed to have implicitly approved that Request and as such, will have their Delivery State set to QUEUED, their Approval State set to APPROVED, and their State Type set to ACTIVE. The entity will, however, retain rights to set their Approval Status (i.e., if they wish to deny their own Request, they may do so).

Entities with Approval Rights on a Request are specifically instructed to take action on the e-Tag through the use of the ApprovalRights flag.

3.6.2.1 Distributing a New e-Tag Request

Distribution of a New e-Tag Request is handled as described in Section 3.6.2.

3.6.2.2 Distributing a Correction Request

Distribution of a Correction Request is handled as described in Section 3.6.2.
For entities impacted by the Request, the Authority must set the IMPACT flag to TRUE.
For entities not impacted by the correction, the IMPACT flag must be set to FALSE.
In certain situations, it is possible for a Transmission Customer or Scheduling Entity to be added or removed. Should such a case occur, the following process must take place:

1. Any Entities being removed must be sent the correction with the impact flag set to TRUE
2. Any Entities being removed must have their entries removed from the Distribution list

3. Any Entities being removed must have their entries removed from the RequestApprovalRights list
4. Any New Entities must have their entries added to the Distribution list
5. Any new customers must have their entries added to the RequestApprovalRights list.

Following the completion of these steps, the Correction must be distributed normally.

3.6.2.3 Distributing a Profile Change Request

All distributions must include the market levels or reliability limit profiles for that period.

Distribution of a Profile Change Request is handled as described in Section 3.6.2. If a Reliability Limit Clearing is being requested, then that limit clearing must be distributed to all entities.

3.6.3 Request Actions

3.6.3.1 Processing Request Approvals and Denials

The following validation criteria must be checked when an Authority receives a Request Approval or Denial message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag Id presented must represent an e-Tag currently held by the Authority
- The Request ID presented must represent a Request currently held by the Authority
- The Security Key presented must be identical to the key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The entity attempting to set State must be one of the entities having approval rights over the Request.
- An Author of the State Setting must be specified
- State Settings are only allowed for Requests that are not in a final state.
- State Settings of DENIED or STUDY must be accompanied by reasons that explain why the specific state was chosen
- The entity attempting to set State must have the most recent correction of the data within its scope

Once a Request Approval message passes validation, the Authority must store the State in its local data store and use it to identify when the Request's Approval State should be updated. The State Type must be marked as "ACTIVE." If a denial or study, the State information must be distributed to all parties.

In certain cases, the Authority Operator may be obligated to override a State request on the behalf of another entity. Should this situation occur, the new State must be recorded and the State Type set to "OVERRIDE."

3.6.3.2 Processing a Withdraw Request

The following validation criteria must be checked when an Authority receives a Withdraw Request message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag ID presented must represent an e-Tag currently held by the Authority
- The Request ID presented must represent a Request currently held by the Authority.
- The Security Key presented must be identical to the key associated with the Profile Change requester. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, the key will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The entity attempting to Withdraw must be the Author of the Request.
- A Withdrawal is only allowed for a Request that is PENDING
- A Withdrawal must be accompanied by a reason that explains why the Withdrawal was made.
- Withdraw Requests may be submitted for ATF Requests that have a Request State of PENDING

If the Request State of the Request is PENDING, then the Authority must set the Request State of the Request to WITHDRAWN and distribute a DistributeStatus message as required in section 3.6.4.

WITHDRAWN is a final state.

3.6.3.3 Processing a Terminate Request

The following validation criteria must be checked when an Authority receives a RequestTerminateTag message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag ID presented must represent an e-Tag currently held by the Authority
- The Security Key presented must be identical to the key associated with the Profile Change requester. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, the key will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- RequestTerminateTag requests are only allowed for e-Tags that are CONFIRMED, IMPLEMENTED, or TERMINATED.

- The RequestTerminateTag request must contain a termination time that is between the e-Tag block start time and e-Tag block end time, and later than the time of receipt.
- A RequestTerminateTag request is invalid if it requests a start time that is later than or equal to an existing RequestTerminateTag Request for the same e-Tag; however, a request for an earlier termination time is allowable.
- Upon the RequestTerminateTag request becoming APPROVED, all PENDING RequestProfileChange requests with block end time after the termination time, and all PENDING RequestTerminateTag requests with termination time after the APPROVED Request's termination time, must be set to a Request State of DENIED.

The Authority must distribute a DistributeTerminate message as defined in 3.6.1.1.1. The Request is subject to the same approvals as a new adjustment request. The Authority sets the ActOnByTime based on the receipt time of the message and the NERC/NAESB Interchange Standard timing tables. This will also include calculation of ramp start time. The Authority also sets the TimeClassification based on the NERC/NAESB Interchange Standard timing tables and the termination time. If the Request State becomes APPROVED, the Authority's action depends on the termination time.

- If the termination time is equal to the block start time of the e-Tag, then the Authority must distribute a DistributeResolution message that sets the Composite State of the e-Tag to CANCELLED.

- If the termination time is after the block start time of the e-Tag, then the Authority must set the market level profiles and transmission allocation profiles of the e-Tag to zero starting at the termination time, and distribute a DistributeResolution message that includes the time at which the Authority intends to set the e-Tag's Composite Status to TERMINATED. This is called the TerminationTime.

CANCELLED and TERMINATED are final states.

3.6.4 Information Distribution

Whenever a significant status event occurs as defined below, or a Request Resolution occurs, the Authority must notify all parties on the distribution list of the e-Tag regarding the change. This notification aids in coordination and communication between the various entities involved with the transaction. These notifications follow the same procedure used by the other Request Distribution messages, described in section 3.6.2.

3.6.4.1 Distribution of Request Approval State

A significant status event (an event triggering a State Distribution) is defined as one of the following:

- An Approver sets their State to DENIED, STUDY or APPROVED
- The Authority sets a Delivery state to INVALID or COMMFAIL

The distribution must contain the State of ALL entities with approval or viewing rights over the Request.

When a distribution is triggered, the Authority must wait five (5) seconds to verify no other changes are made to the States associated with the Request. If such changes are made, the distribution must be updated to include those changes. If the Denial or Study is overridden to APPROVED, the distribution must be aborted.

Distribution of a Request Approval State is handled as described in Section 3.6.4.

3.6.4.2 Distribution of Request Resolution

The events triggering a Request Resolution Distribution are as follows:

- All Approvers have set their State to Approved, or
- The time for approval of the Request expires, or
- A requester withdraws the Request.

Given the above events, the following rules apply to determining the resolution of the Request:

- If a requester has withdrawn the Request, the Request is WITHDRAWN.
- If all approvers have set their State to Approved, the Request is APPROVED and the Composite State is CONFIRMED.
- If time has expired and any Approver' current State is DENIED, the Request is DENIED.
- If time has expired, and no Approver's current State is DENIED, and all Reliability Entity's current State is APPROVED, the Request is APPROVED.
- The individual status of any Market Entity whose current State is PENDING will be set to APPROVED and the Type will be set to PASSIVE when the Request State of the Request is APPROVED.
- If time has expired, and any Reliability Entity's current State is EXPIRED (or PENDING), the Request is EXPIRED.

When the Authority distributes a Request Resolution for a New e-Tag Request where the Composite State of the e-Tag is transitioning to CONFIRMED, the Authority must calculate and distribute the "ImplementTime" so that all Agent and Approval services know when the Authority is planning to make the transition from CONFIRMED to IMPLEMENTED.

Distribution of a Request Resolution is handled as described in Section 3.6.4.

3.6.4.3 Potential TLR Profile Change Distributions

The Authority has no requirements with regard to the Distribution of Potential TLR Profile Changes.

3.6.5 Recovery Functions

3.6.5.1 Processing Synchronous Queries

Synchronous Queries include the following:

- QueryTag
- QueryRequestIDs
- QueryRequest
- QueryStatus
- QueryAvailability

The following procedure should be used to process all synchronous queries:

- Decode the XML message and perform syntactic/semantic validation
- If the query passes validation return the requested data. Otherwise return a fault or error message

3.6.5.1.1 Processing an e-Tag Query

The following validation criteria must be checked when an Authority receives a Query e-Tag message:

- The e-Tag ID Referenced in the message must be one held by the Authority
- The Security Key presented must be identical to the key associated with the querying party and must be associated with the e-Tag being queried. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, this will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The rules described in the Data Model and Method Descriptions sections must not be violated.

3.6.5.1.2 Processing a Request Ids Query

The following validation criteria must be checked when an Authority receives a Query Request Ids message:

- The e-Tag ID Referenced in the message must be one held by the Authority
- The Security Key presented must be identical to the key associated with the querying party and must be associated with the e-Tag being queried. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, this will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The rules described in the Data Model and Method Descriptions sections must not be violated

Once a Request IDs Query message passes validation, the authority should return the requested data ordered by Request State and then by Request creation time (oldest to most recent).

3.6.5.1.3 Processing a Request Query

The following validation criteria must be checked when an Authority receives a Query Request message:

- The e-Tag ID Referenced in the message must be one held by the Authority
- The Security Key presented must be identical to the key associated with the querying party and must be associated with the e-Tag being queried. For the e-Tag Author this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers this will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The rules described in the Data Model and Method Descriptions sections must not be violated

3.6.5.1.4 Processing a Request State Query

The following validation criteria must be checked when an Authority receives a Query Request State message:

- The e-Tag ID Referenced in the message must be one held by the Authority
- The Security Key presented must be identical to the key associated with the querying party and must be associated with the e-Tag being queried. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, this will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The rules described in the Data Model and Method Descriptions sections must not be violated

3.6.5.1.5 Processing Queries for System Availability

Authorities should respond back to Queries for System Availability as follows:

- If the Authority is operating correctly, the Return Value should be SUCCESS.
- If the Authority is not operating correctly, the Return Value should be FAIL.
- If a known error is occurring, the Authority should indicate that error.

3.6.5.2 Processing Asynchronous Queries

Asynchronous Queries include the following:

- QuerySummaries
- QueryTags
- QueryHistory

The following procedure should be used to process all asynchronous queries:

- Decode the XML message and perform syntactic/semantic validation
- If the query passes validation, queue the Request for further processing and return a success response, otherwise return a fail response.

- Periodically read and process all queued queries. For each query, send a new (callback) message to the registered URL of the party that submitted the query. The callback message should contain the data that was requested by the previous Query message.
- If the callback message fails or encounters a fault response, attempt to resend the message using the process described in section 7.1.1.1.

3.6.5.2.1 Processing e-Tag Summary Queries

The following validation criteria must be checked when an Authority receives a Query e-Tag Summary message:

- The Range specified for the query must not exceed twenty-four (24) hours. Systems may, at their option, reject any single query that indicates a desire for more than 24-hours of information.
- The rules described in the Data Model and Method Descriptions sections must not be violated

Once an e-Tag Summary Query message passes validation, the authority should return the requested data ordered from oldest to most recent based on the users search criteria (Date Active or Date Modified). The security key used for the callback message should be the same security key that was used when the e-Tag Summary Query message was submitted.

When an approval or agent service requests recovery over an outage range, the service must create a list of unique URL's for Authority services and send the Query Summary messages to each authority service in order to retrieve all e-Tags for which that e-Tag approval or agent service is a party. For Authorities that are shared between multiple companies, only one QuerySummaries message is required. The Tag Authority should return data for all tags that are visible to the requestor in this case, regardless of which the Authority's companies is listed as the intended message recipient.

3.6.5.2.2 Processing an e-Tags Query

The following validation criteria must be checked when an Authority receives a Query e-Tags message:

- The e-Tag Ids presented must be held by the Authority
- The e-Tag Keys associated with those e-Tag Ids must be valid keys associated with those e-Tags and with the querying entity
- The Return Rate must be greater than zero (0)
- The rules described in the Data Model and Method Descriptions sections must not be violated

Once a Query e-Tags message passes validation, the authority should return the requested data ordered by e-Tag creation time from oldest to most recent. Each callback message should contain one or more e-Tags, but not more than the number of e-Tags specified in

the Return Rate field of the Query e-Tags message. Each message may contain fewer than the requested number of e-Tags. The security key used for the callback message should be the same security key that was used when the e-Tag Summary Query message was submitted.

3.6.5.2.3 Processing an e-Tag History Query

The following validation criteria must be checked when an Authority receives a Query e-Tag History message:

- The TagID Referenced in the message must be one held by the Authority
- The Security Key presented must be identical to the key associated with the querying party and must be associated with the queried e-Tag. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, this will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- The rules described in the Data Model and Method Descriptions sections must not be violated
- The Authority should return all data to the caller, regardless of the message delivery status, except for retry messages (which should never be returned).

Once a Query e-Tags message passes validation, the authority should return the requested data ordered by Call Time Stamp (oldest to most recent).

3.7 Availability and Performance

Availability and performance requirements are specified in NERC/NAESB Standards, as well as a description of what actions to take during a system outage to ensure transaction of business is not halted.

Section 4 - Tag Approval Functional Requirements

4.1 Introduction

All entities that may have "approval rights" over any Interchange Transaction shall provide the necessary hardware and software systems to implement the Approval. The Approval shall comply with all functional requirements set forth in this section. Approval entities may elect to comply with these Approval requirements using internally developed hardware/software; third party developed hardware/software, or third party subscription type services.

Approval shall be responsible for providing the following functions:

- Accept input e-Tag data transferred in compliance with this document from any Authority.
- Provide immediate syntactical validation of the incoming data stream and respond accordingly (i.e., provide for positive acknowledgement of receipt of the e-Tag).
- Communicate approval, denial, study, and adjustment information to the Authority managing the e-Tag in compliance with this document.
- Receive notification messages from the Authority.
- Query the appropriate Authority for the current State of each Request submitted for approval.

Information systems designed to provide more than one electronic e-Tagging service (e.g., Authority and Approvals) are free to use any internal or proprietary mechanisms to convey e-Tag information between those functional services, but must still comply with all technical standards and protocols related to the exchange of transaction information with e-Tagging related services provided by (or for) others.

4.2 Registry Usage

The Approval shall be responsible for maintaining an updated list of all registered PSEs, Transmission Service Providers (TSPs), Balancing Authorities (BAs), and any other such entities whose identities must be uniquely specified in connection with the arrangement of an Interchange Transaction. The Electric Industry Registry of all such entities shall be maintained and available for downloading from the Electric Industry Registry web site. The Approval shall supply a procedure to allow updates from the Electric Industry Registry on demand or on a prescheduled interval. The Electric Industry Registry shall be maintained in a format defined by the NERC/NAESB Joint Interchange Scheduling Working Group.

The Approval must support the receipt of unsolicited messages sent by Authorities. To enable the delivery of these messages, the user must register the appropriate service identification information in the Electric Industry Registry and be capable of receiving e-Tag messages.

4.3 Tag Data Entry and Viewing

The Approval is the main interface through which entities with approval rights to an e-Tag alert the e-Tag author and each other of their decisions to approve, deny, or change an e-Tag to reflect a valid representation of a scheduled transaction. To this end, the Approval shall provide a mechanism for a user to view, make changes, or modify the entity state(s), as well as perform all other functional requirements described herein. The exact nature of this user interface is beyond the scope of this document; with the exception that the user shall have the facilities to view all transaction related information (as described in the Data Model) necessary to represent a complete, valid e-Tag.

4.4 Date and Time Handling

The Approval shall be responsible for the conversion of all date and time related input fields to Universal Coordinated Time (UTC) prior to information being exchanged with any other service. Valid times during the day shall be from 00:00:00 to 23:59:59. The Approval user interface is free to accept and manage the conversion of any appropriate date/time formats at the discretion of the service provider. The internal representation of date and time within the Approval is also entirely at the discretion of the service provider. However, all electronic transmittal of data shall be in UTC time.

4.5 Data Validation

The Approval shall ensure that all data elements in a communication are legitimate and that no syntax or validation rules have been broken.

4.6 Function Implementation

The Approval is responsible for being able to call the following methods:

- RequestCorrection
- RequestProfileChange
- SetState
- WithdrawRequest
- QuerySummaries
- QueryTag
- QueryTags
- QueryHistory
- QueryRequestIDs
- QueryRequest
- QueryStatus
- QueryAvailability

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeTerminateTag
- DistributeProfileChange
- DistributeStatus

- DistributeResolution
- CallbackSummaries
- CallbackTags
- CallbackHistory
- QueryAvailability

Semantics, including calling and processing rules are described in detail in the following sections.

4.6.1 Initiating a Request

The Approval may only issue one type of Request – the Profile Change Request. The following procedure should be used to validate and process a new e-Tag Creation request:

- Write the new Request and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.

4.6.1.1 Submitting a Correction Request

Write Request – Transmission Service Providers (TSPs) may submit e-Tag correction(s) if needed. The TSP must also provide any additional parameters necessary to successfully call the RequestCorrection method. The Approval may elect to automate the provision of some of these parameters (i.e., Security Key, e-Tag Code, etc…). When submitting a correction, the correction must contain all the necessary data to replace the existing data. For example, a correction to a TransProductRef must not only contain the TransProductRef, but also the Transmission Allocation ID, a reference to the Parent Segment, the OASIS Number, and the associated Transmission Customer.

The TSP is only allowed to modify the TransProductRef and transmission allocation on a physical segment where they are the associated TSP (TPCode). The TSP may horizontally or vertically stack transmission, just as the e-Tag Author can, however the total transmission allocation may not be changed (either reduced or increased)

Verify Semantics – the following rules must be met in order to constitute a valid Request:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Corrections may only be made to e-Tags that are PENDING

- Corrections may not be made that violate the rules defined in NERC/NAESB Standards regarding appropriate use of correction

Should the Request not be valid, the TSP must be informed of the error(s) by the Approval and provided with an opportunity to rectify the violation.

Store Reference Number – The Authority will assign each correction a number that is used to indicate the most recent correction to be applied to a specific segment or allocation (or set of such changes). The Approval must record these numbers for later reference and integrity verification.

4.6.1.2 Submitting a Profile Change Request

When requesting a setting of the reliability limit, the Approver may specify the profile at a specific physical segment. If the Approver does not specify a physical segment the default is the generator. The Authority will calculate the remaining profiles for all other upstream and downstream profiles. The Approver must provide any additional parameters necessary to successfully call the RequestProfileChange method. If requesting a clearing of reliability limits, the Approver must specify a start and a stop range for the clearing of the limit. Approvals are not allowed to submit Current Level profiles, as they are calculated by the Authority.

The Approval may elect to automate the provision of some of these parameters (i.e., Security Key, e-Tag Code, etc…).

In some cases the Market Operators may specify Market Level Profile changes rather than Reliability Limit Profile Changes. Specifying a Market Level Profile Change is completely acceptable provided the entity is a registered Market Operator and the Profile Change Request would modify a transaction that sources or sinks in the Market Operator's Balancing Area(s). Such use of the Market Level profile must ONLY be used by the Market Operator when market conditions are setting the flow of the transaction; reliability concerns must still be handled through the use of the Reliability limit. Market Operators must provide full sets of profile changes (i.e., not only the profile at the Generator, but all profiles along the scheduling path as well).

In the case of DYNAMIC e-Tags, the sink BA or source BA may specify limit clearing and Market Level Profile changes. This is intended to allow the LCA or GCA to set the energy level of the e-Tag to the metered (actual) interchange value. This type of modification is allowed ONLY for historic data up to 168 hours in the past. When any entity changes a market level, they must also supply all of the profiles in the e-Tag. Changes to the reliability limit, with the exception of limit clearing, must not be allowed for DYNAMIC e-Tags if they are for a period more than one hour in the past.

The TSP may also submit a Market Level Profile change and is only allowed to modify the TransProductRef and transmission allocation on a physical segment where they are the associated TSP (TPCode). The TSP may horizontally or vertically stack

transmission, just as the e-Tag Author can, however the total transmission allocation MWlevel may not be changed (either reduced or increased) nor the earliest start and end times.

The following validation criteria must be checked when an Approval Service creates a Profile Change request message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Profile Changes may only be made to e-Tags with Composite States of CONFIRMED or IMPLEMENTED
- Profile Changes are not allowed for ATF e-Tags (they may be terminated)
- The Profile Changes must not affect points in time more than one (1) hour in the past with the exception of DYNAMIC e-Tags which must not affect points in time more than 168 hours in the past.

It is possible for a TSP to supply changes to the transmission allocation when specifying a profile change. The following rules should be noted:

- It is impossible to delete a transmission allocation. If a reservation needs to be eliminated, its profile must be adjusted to zero.
- A new transmission allocation may be added at any time. This addition will result in the creation of a new reservation allocation and new Base Profile. The transmission allocation will NOT be added as an Exception Allocation since a previous Base Profile does not exist. (See section 6.2.5 for more information on Allocation Profiles.). Transmission allocation IDs must not be re-used, regardless of Request State.
- Should the TSP need to modify a transmission allocation then the TSP must specify the change in the same manner in which profile change would be performed.
- The TSP may not submit a transmission allocation change that modifies the pre-existing transmission allocation MWlevel for any period. Extension is prohibited.
- The adjustment cannot impact any MWlevel or Product in the past. Changes are bound in time with the earliest possible change starting at the time the Authority receives the Request and the latest possible change ending at the Tag Stop Time.

4.6.2 Request Distribution

The following procedure should be used to process all Request Distribution messages:

- Decode the XML message
- Perform any required validations
- If the Request Distribution passes validation, then return a success response, otherwise return fault or error as appropriate.

4.6.2.1 Processing a New e-Tag Request Distribution

Verify Semantics – the following rules must be met in order to constitute a valid New e-Tag Request Distribution:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- A e-Tag with the ID presented must not already exist on the Approval
- An e-Tag designated as ATF must be clearly identifiable. The Approval user interface must be designed so that ATF e-Tags are differentiated/highlighted by color, text, or some other mechanism that ensures the e-Tag Approver is aware that the e-Tag is ATF.

4.6.2.2 Processing a Correction Request Distribution

The following validation criteria must be checked when an Approval Service receives a Distribute Correction message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Corrections may not be made to e-Tag creation Requests that do not have an Approval State of PENDING.
- Corrections may not be made that violate the rules defined in NERC/NAESB Standards regarding appropriate use of correction

Upon receipt of a valid Correction Request Distribution, the Approval must take the following actions:

- Immediately replace the previously received information with the corrected information
- Alert the e-Tag Approver that the correction has occurred, highlighting the correction for their inspection
- Immediately consider any previous approval action (setting the approval State of the affected entity to either APPROVED, DENIED, or STUDY) to be reset

4.6.2.3 Processing a Profile Change Request Distribution

The following validation criteria must be checked when an Approval Service receives a Distribute Profile Change message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Profile Changes may not be made to e-Tags that have not been CONFIRMED or IMPLEMENTED

4.6.3 Request Actions

The following procedure should be used by approval services when taking actions on requests:

- Encode the message in a valid XML format (as described by the latest e-Tag schema).

- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.

4.6.3.1 Approving and Denying Request

The e-Tag Approver must indicate their decision to support or refute the Request. Valid Approval States are defined in Section 1.3.4.2. States of Denied and Study MUST be accompanied with reasons for the choice. States of Approved MAY be accompanied with reasons or comments. The Approver must specify the Request ID that is being acted upon, and must include their assigned Security Key in order for the SetState method call to be processed correctly.

The following validation criteria must be checked when aApproval Service sends a Set Approval State message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The SetState call may not reference any Request that has already been resolved (i.e. has a current final state).
- States of Denied and Study must be accompanied by a reason
- The version of data being corrected must be the most recent correction held by the Authority

4.6.3.2 Withdrawing a Request

Approval services may withdraw profile change requests.

The following procedure should be used to withdraw a Request:

- Write the withdraw message and encode it in a valid XML format (as described by the latest e-Tag schema). The Message must include the following items:
  - The Request ID provided by the Authority at the time the request was made.
  - The original Security Key for the transaction that was used in the e-Tag Creation message.
  - A reason that explains why the Withdrawal was made.
- Withdraw messages must not be sent for requests that have already reached a final state (APPROVED, etc.).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.

- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- WITHDRAWN is a final states for the Request.

4.6.4 Approval Service Information Distribution

4.6.4.1 Processing a Request Approval State Distribution

The following validation criteria must be checked when an Approval Service receives a Distribute Status message:

- The e-Tag ID Referenced in the message must be one held by the Approval
- The Security Key presented must be identical to the original Security Key assigned at the time the Authority initially transferred the New e-Tag Request to the Approval
- The rules described in the Data Model and Method Descriptions sections must not be violated

4.6.4.2 Processing a Request Resolution Distribution

The following validation criteria must be checked when an Approval Service receives a Distribute Resolution message:

- The e-Tag ID Referenced in the message must be one held by the Approval
- The Security Key presented must be identical to the original Security Key assigned at the time the Authority transferred the New e-Tag Request to the Approval
- The rules described in the Data Model and Method Descriptions sections must not be violated

4.6.4.3 Potential TLR Profile Change Distributions

The Approval has no requirements with regard to the Distribution of Potential TLR Profile Changes.

4.6.5 Recovery Functions

4.6.5.1 Synchronous Queries

Synchronous Queries include the following:

- QueryTag
- QueryRequestIDs
- QueryRequest
- QueryStatus
- QueryAvailability

The following procedure should be used to initiate all synchronous queries:

- Write the query and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP POST message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.

4.6.5.1.1 Query for an e-Tag

Tag approval service must specify a valid e-Tag ID and the associated Security Key they were assigned when given the original New e-Tag Request.

4.6.5.1.2 Query for Request Ids

Tag approval service must specify a valid e-Tag ID and the associated Security Key they were assigned when given the original New e-Tag Request. Optionally, the user may elect to filter RequestID's based on the resolution of the requests associated with the e-Tag (i.e., show only Activates Requests).

4.6.5.1.3 Query for a Request

Tag approval service must specify a valid e-Tag ID and the associated Security Key they were assigned when given the original New e-Tag Request, as well as the Request ID they wish to retrieve.

4.6.5.1.4 Query for a Request's State

Tag approval service must specify a valid e-Tag ID and the associated Security Key they were assigned when given the original New e-Tag Request, as well as the Request ID for which they would like State information.

4.6.5.1.5 Query for System Availability

Tag approval service must specify a particular system for which to query availability (by entity desk and service type (Agent, Approval, Authority, RAS).

4.6.5.1.6 Processing Queries for System Availability

Approvals should respond back to Queries for System Availability as follows:

- If the Approval is operating correctly, the Return Value should be SUCCESS.
- If the Approval is not operating correctly, the Return Value should be FAIL.
- If a known error is occurring, the Approval should indicate that error.

4.6.5.2 Asynchronous Queries

Asynchronous Queries include the following:

- QuerySummaries

- QueryTags
- QueryHistory

The following procedure should be used to initiate all asynchronous queries:

- Write the query and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag, or, for Query Summaries, identify a unique list (select distinct) of Authority URL's. Send the XML message(s) created during the first step to this/these URL(s) as the payload of an HTTP POST message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.
- Wait for a response message(s) from the Authority. The response message(s) will be over a new HTTP connection (not part of the query submission described in previous steps). The response will be sent to the Approval Service's registered service URL, and will include the same security key used by the Agent to submit the query. The Agent should perform syntactic and semantic validation on the query response message from the Authority, and reply to the query response message with either a success reply or a Fault/Error reply.

4.6.5.2.1 Query Summaries

The approval service must specify either an Active Range or a Last Modified Range for which they want e-Tag summaries to be returned. The Active Range is used to specify a range of time during which an e-Tag must have been "active" (i.e., either the first start date/time pair or the last stop date/time pair of the e-Tag is within the Active Range). The Last Modified Range is used to specify a range of time during which the e-Tag had a request made against it (New e-Tag Requests, Correction Requests, and Profile Change Requests).

When an approval or agent service requests recovery over an outage range, the service must create a list of unique URL's for Authority services and send the Query Summary messages to each authority service in order to retrieve all e-Tags for which that e-Tag approval or agent service is a party. For Authorities that are shared between multiple companies, only one QuerySummaries message is required. The Tag Authority should return data for all tags that are visible to the requestor in this case, regardless of which the Authority's companies is listed as the intended message recipient.

The User must also generate and specify a Security Key with which the Callback can be secured.

The following validation criteria must be checked when an Approval Service submits a Query Summaries message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The Range specified must not exceed twenty-four (24) hours. Systems may, at their option, reject any single query that indicates a desire for more than 24-hours of information.

The following validation criteria must be checked when an approval service receives a Query Summaries Callback message:

- The Security Key presented must be identical to the original Security Key provided at the time the Approval transferred the Summaries Query to the Authority
- The rules described in the Data Model and Method Descriptions sections must not be violated

4.6.5.2.2 Query e-Tags

The Agent service must provide a list of e-Tag IDs and Security Keys for all e-Tags to be queried. Agent must also specify a Return Rate, which indicates how many e-Tags the Agent wishes to receive within each callback. Missing security keys can be recovered using the Query Summaries message. The User must also specify a separate Security Key for the query with which the Callback can be secured.

Special Note: Query e-Tags may return more than one callback, depending on how the user configures their original query and how the Authority is configured.

The following validation criteria must be checked when an Agent receives a Query e-Tags Callback message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag IDs presented must match the e-Tag IDs requested in the original query
- The Security Key presented must be identical to the original Security Key provided with the original query

4.6.5.2.3 Query History

The Approval Service must specify a valid e-Tag ID and Security Key. The security key should be the same key that was used when creating the e-Tag (for e-Tag authors), or the security key provided by the Authority through a Distribute message. Missing security keys can be recovered using the Query Summaries message.

The following validation criteria must be checked when an Approval Service receives a Query History Callback message:

- The e-Tag ID presented must match the e-Tag ID requested in the original query
- The Security Key presented must be identical to the original Security Key provided with the original query
- The rules described in the Data Model and Method Descriptions sections must not be violated

4.7 Availability and Performance

Availability and performance requirements are specified in NERC/NAESB Standards, as well as a description of what actions to take during a system outage to ensure transaction of business is not halted.

Section 5 - Reliability Authority Service

5.1 Introduction

RASs are used by Reliability Coordinators (RCs) to identify transactions for curtailment, reallocation, and reloading. Functions of a RAS with regard to Reliability Authority and operations are determined by the NERC IDC Working Group or other industry groups. The information below describes the role of a RAS with regard to the e-Tag system.

5.2 Registry Usage

RASs shall be responsible for maintaining an updated list of all registered PSEs, Transmission Service Providers (TSPs), Balancing Authorities (BAs), and any other such entities whose identities must be uniquely specified in connection with the arrangement of an Interchange Transaction. The Electric Industry Registry of all such entities shall be maintained and available for downloading from the Electric Industry Registry web site. RASs shall supply a procedure to allow updates from the Electric Industry Registry on demand or on a prescheduled interval. The Electric Industry Registry shall be maintained in a format defined by the NERC/NAESB Joint Interchange Scheduling Working Group. RASs must support the receipt of unsolicited messages sent by Authorities. To enable the delivery of these messages, the user must register the appropriate service identification information in the Electric Industry Registry and be capable of receiving e-Tag messages.

5.3 e-Tag Data Entry and Viewing

User Interface rules for RASs are defined by the NERC IDC Working Group or other industry groups.

5.4 Date and Time Handling

RASs shall be responsible for the conversion of all date and time related input fields to Universal Coordinated Time (UTC) prior to information being exchanged with any other service. Valid times during the day shall be from 00:00:00 to 23:59:59. RASs' user interfaces are free to accept and manage the conversion of any appropriate date/time formats at the discretion of the service provider. The internal representation of date and time within the RAS is also entirely at the discretion of the service provider. However, all electronic transmittal of data shall be in UTC time.

5.5 Data Validation

RASs shall ensure that all data elements in a communication are legitimate and that no syntax or validation rules have been broken.

5.6 Function Implementation

The RAS is responsible for being able to call the following methods:

- RequestProfileChange
- SetState
- DistributePotentialTLRProfileChange

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeProfileChange
- DistributeResolution

Semantics, including calling and processing rules are described in detail in the following sections.

5.6.1 Initiating a Request

Reliability Authority services may only issue one type of Request – the Profile Change Request. The following procedure should be used to validate and process a new e-Tag Creation request:

- Write the new Request and encode it in a valid XML format (as described by the latest e-Tag schema).
- Look up (in the Electric Industry Registry) the Authority URL associated with the load control area on the e-Tag. Send the XML message created during the first step to this URL as the payload of an HTTP message, and wait for the response.
- If the submission fails or the response contains fault or error messages, do not automatically retry the submission. Log the error and correct the problem before attempting resubmission. If the response succeeds, then process any data returned by the Authority.

5.6.1.1 Submitting a Profile Change Request

The following validation criteria must be checked when a RAS creates a Profile Change request message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Profile Changes may **only** be made to e-Tags that have been CONFIRMED or IMPLEMENTED
- The Profile Changes must not affect points in time more than one (1) hour in the past with the exception of DYNAMIC e-Tags, which must not affect points in time more than 168 hours in the past.

5.6.2 Request Distribution

The following procedure should be used to process all Request Distribution messages:

- Decode the XML message
- Perform any required validations
- If the Request Distribution passes validation, then return a success response, otherwise return fault or error as appropriate.

5.6.2.1 Processing a New e-Tag Request Distribution

The following validation criteria must be checked when a RAS receives a Distribute New e-Tag message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- An e-Tag with the ID presented must not already exist on the RAS

5.6.2.2 Processing a Correction Request Distribution

The following validation criteria must be checked when a RAS receives a Distribute Correction message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Corrections may not be made to e-Tags that do not have a Composite State of PENDING.
- Corrections may not be made that violate the rules defined in NERC/NAESB Standards regarding appropriate use of correction

5.6.2.3 Processing a Profile Change Request Distribution

The following validation criteria must be checked when a RAS receives a Distribute Profile Change message:

- The rules described in the Data Model and Method Descriptions sections must not be violated
- Profile Changes may not be made to e-Tags that have not been CONFIRMED or IMPLEMENTED

5.6.3 Information Distribution

5.6.3.1 Processing of a Request Resolution Distribution

The following validation criteria must be checked when an Approval Service receives a Distribute Resolution message:

- The e-Tag ID Referenced in the message must be one held by the RAS
- The Security Key presented must be identical to the NERC-assigned Security Key for RAS communications.
- The rules described in the Data Model and Method Descriptions sections must not be violated

5.6.3.2 Distribution of a Potential TLR Profile Change

Note – The following actions describe the role of the NERC Interchange Distribution Calculator (IDC) with regard to the generation of curtailment prescriptions. While other RASs may choose to implement this feature, it is not strictly required.

The following procedure should be used to initiate all asynchronous queries:

- Write the query and encode it in a valid XML format (as described by the latest e-Tag schema).

- Look up (in the Electric Industry Registry) the Agent URL associated with the PSE listed as the e-Tag author for the e-Tag impacted by the Potential TLR profile change

Agents may implement a callback mechanism to verify validity of the distribution, but are not required to do so.

The following validation criteria must be checked when a RAS receives a Potential TLR Profile Change callback message:

- The Security Key presented must be identical to the original Security Key provided at the time the RAS transferred the Potential TLR Profile Change to the Agent
- The rules described in the Data Model and Method Descriptions sections must not be violated

5.7 Availability and Performance

Availability and Performance Requirements for the RASs are defined by the NERC IDC Working Group or other industry groups.

Section 6 - Data Model Overview

6.1 Tag Data

6.1.1 Transaction Types

E-Tag 1.7 recognizes the following transaction types:
Normal: These are the "normal energy schedules" and should be the largest number of schedules. They will include schedules that use point-to-point, network integrated transmission service, or grand-fathered service under a regional tariff. These schedules are included in the IDC and are subject to TLR curtailment.
Dynamic: A dynamic schedule is scheduled using an expected value but the actual energy transfer is determined in real time by separate communications external to the e-Tag system. Also included in this type will be regulation energy schedules and energy imbalance schedules. The e-Tag should contain the expected average energy in the energy profile and contain the maximum expected energy in the transmission allocation. Dynamic e-Tags may be adjusted by the source BA, sink BA, or e-Tag author up to 168 hours in the past using a market adjust to set the actual interchange value.
Emergency: Emergency Schedules, including reserve sharing, Spinning Reserve, and Supplemental Reserve may be scheduled as Emergency Schedule Type. Another kind of emergency schedules is execution of an operating guide that implements schedules in response to a loading problem. For example, an RTO based emergency re-dispatch that lasts longer than an hour involving multiple Balancing Authorities. Typically, EMERGENCY schedules would not require reservations before being used where Capacity Benefit Margin had been calculated to allow for this reserve sharing.
Loss Supply: Used for customers self-supply losses. This type is used to differentiate between a loss schedule and a normal schedule. Some tariffs presently require that schedules for losses require different treatment than schedules for the associated energy.
Capacity: Typically used for entities to import operating reserves from outside their reserve-sharing group but may also be used to arrange for purchases or sales of Spinning Reserve and Supplemental Reserve between other entities. This type of e-Tag may be activated upon contingency with zero ramp durations.
Pseudo-Tie: A dynamic transfer implemented as a pseudo-tie rather than a dynamic schedule. Used in the same way as a Dynamic e-Tag. These tags may be adjusted in the same manner as Dynamic transaction type e-Tags.

6.1.2 Market Segments

Market Segments represent those portions of the path that are associated with the tracking of title and responsibility. A Physical Segment is always associated with a parent Market Segment. However, the opposite is not true; Market Segments can exist independent of Physical Segments.
Market Segments contain information that describes the market information, such as the identity of the market participant, the firmness of energy the market participant is delivering, and the physical segments the entity is responsible for providing. Market Segments must be listed in order from GPE to LSE and numerically identified as such (e.g., GPE segment = 1, Intermediate PSE segment =2, LSE segment = 3).

GPE and LSE segments must contain an energy product. Market Segments may only utilize products in the Electric Industry Registry related to Generation or Load.

6.1.2.1 Scheduling Responsibilities

Market Segments can describe a responsibility for managing the scheduling for a portion of the transaction. This is seen when a marketer has rights to a resource and wishes to exercise those rights (i.e., a generation merchant wishes to generate energy for sale, a load serving entity wishes to consume energy based on a purchase, or a marketer wishes to physically move energy from one area to another). When this occurs, the market segment will contain the physical segments over which the marketer has scope.

6.1.2.2 Title Transfers

Market Segments can also describe non-physical title transfers. These are seen when a market participant takes financial possession for the energy commodity, but does not physically move that energy before transferring possession to another financially responsible party. When this occurs, the market segment will not contain any physical segments.

6.1.3 Physical Segments

Physical Segments represent those portions of the path that are physical in nature and represent a movement of energy. There are three types of physical segment: Generation, Transmission and Load. Physical segments must be listed in order from generation to Load and numerically identified as such (i.e., Generator segment = 1, first TSP segment =2, second TSP segment = 3, Load segment = 4). Generation segments must always be listed first, while Load segments must be listed last. E/*-Tags may only have one Generation segment and one Load segment. All physical segments must reference a parent market segment, identifying the market entity responsible for the physical segment. These references must also be in an order that matches that described by the market segments. For example, the following represents a valid description of a transaction:

GPE: Market Segment 1
PSE: Market Segment 2
LSE: Market Segment 3

Generator: Physical Segment 1, Parent Market Segment Ref 1
Transmission: Physical Segment 2, Parent Market Segment Ref 2
Load: Physical Segment 3, Parent Market Segment Ref 3

In this example, the chain of ownership and physical path are aligned properly. When combined, the results identify a clear tracking of title and scheduling path:

GPE: Generator
PSE: Transmission
LSE: Load

However, the following example is invalid:

GPE: Market Segment 1
PSE: Market Segment 2
LSE: Market Segment 3

Generator: Physical Segment 1, Parent Market Segment Ref 1
Transmission: Physical Segment 2, Parent Market Segment Ref 3
Load: Physical Segment 3, Parent Market Segment Ref 2

In this example, the references indicate a paradox: when combined, invalid results are produced:

GPE: Generator
PSE: Load ←out of sequence
LSE: Transmission ←out of sequence

Such cross references are invalid.

6.1.3.1 Generation

Generation Segments contain information that describes a generation resource, such as the location of the generation, the firmness of the energy supplied by the resource, and contract references that identify the resource commitment. Generation Segments may only utilize products in the Electric Industry Registry related to Generation.

6.1.3.2 Transmission

Transmission Segments contain identification that describes a transmission service, such as the identity of the provider, the POR and POD of the service, the firmness of the service, simple loss information, and contract references that identify the service commitment. Transmission Segments may only utilize products in the Electric Industry Registry related to Transmission.

6.1.3.2.1 Scheduling Entities

Scheduling Entities must be registered as Balancing Authorities in the Electric Industry Registry. Many Transmission Service Providers require that e-Tags illustrate not only the contractual relationship between the Transmission Service Provider and the transmission customer, but also the internal scheduling information to implement the transmission service sold under their tariff. To this end, Scheduling Entities may be defined for a particular Transmission segment. These entities must be listed in the proper scheduling path order (for example, importing BA, intermediate BA, exporting BA).

In the event a listed POR or POD in the Transmission Segment is listed in the Electric Industry Registry as being a DC Tie, then its registered Balancing Authority must be listed in the e-Tag as a scheduling entity.

NERC/NAESB Standards indicates that Scheduling Entities are optional items in an e-Tag. While there is no requirement in this Specification (or the XML Schema associated with it) that Scheduling Entities be listed, it should be noted that NERC/NAESB Standards requires that scheduling paths be contiguous and verified by all scheduling entities before an e-Tag is approved. Failure to include the proper scheduling entities (or failure to include them in the proper order or location) will likely result in a denied e-Tag. e-Tag

6.1.3.3 Load

Load Segments contain information that describes a load, such as the location of the load, the interruptability of the load, and contract references that identify the load obligation. Load Segments may only utilize products in the Electric Industry Registry related to Load.

6.1.4 Profile Sets

Profile Sets define the level at which transactions should run, as well as the factors that set those levels. Profiles are specified as a series of time-ordered segments of duration associated with a particular profile type or types. These segments may be repeated on multiple days, if so desired. Profiles are specified as either *relative* or *absolute*, depending on the type of profile.

A *Relative* profile is described through the use of two or more values which, when combined, create a matrix of profiles. For example, a relative profile may specify a set of reference date-times (01/01/2001 06:00:00, 01/02/2001 06:00:00,) and a set of offsets relative to that date-time (00:00, 02:00, and 04:00). When multiplied together, the resultant matrix is as follows:

	01/01/2001 06:00:00	*01/02/2001 06:00:00*
00:00	**01/01/2001 06:00:00**	**01/02/2001 06:00:00**
02:00	**01/01/2001 08:00:00**	**01/02/2001 08:00:00**
04:00	**01/01/2001 10:00:00**	**01/02/2001 10:00:00**

Doing so reduces the size of the data significantly (in this case, instead of six explicit date times, only two explicit date times must be supplied, along with three simple time offsets).

An *Absolute* profile is described through the use of explicit date times. The above example, defined through absolute profiles, would be as follows:

01/01/2001 06:00:00
01/01/2001 08:00:00
01/01/2001 10:00:00
01/02/2001 06:00:00
01/02/2001 08:00:00
01/02/2001 10:00:00

While more verbose, the use of such profiles is more effective when only small profiles are to be specified, or when explicit dates in a relative profile must be referenced.

In all cases, start times must always be earlier than their associated stop times.

Both Relative and Absolute profiles may optionally contain ramp duration (in minutes) associated with both start time and stop time. The ramp stop time is not needed (and is ignored) in any profile except for the last profile. The ramp duration specifies the number of minutes over which the generator will change from the previous block level to the current block level. Interchange schedule ramping is executed between BAs using straddle ramp methods as defined above. The ramp duration exists in the e-Tag in order to provide a vehicle by which ramp duration may be exchanged between entities. Ramps may not overlap. Agent Software, e-Tag Approval Software and Authority software must include at least this validation plus any validation required by NERC, NAESB or RRO standards.

6.1.4.1 Profile Types

There are five main types of profiles: Market Level, Reliability Limit, Dynamic Minimum Energy, Dynamic Maximum Energy, and Current Level.

6.1.4.1.1 Market Level

The Market Level defines the level at which the e-Tag author wishes the transaction to run. This level can be used to specify an initial value for a dynamic schedule, as well as a simple level at which the transaction is to be run.

6.1.4.1.2 Reliability Limit

The Reliability Level defines the maximum allowable level at which a transaction may run when that transaction has been identified by a Reliability Coordinator or other reliability entity as being limited by some constraint. This limit is typically used to indicate curtailments.

6.1.4.1.3 Dynamic Minimum Energy

Dynamic Minimum Energy specifies a level at which a Dynamic Schedule must minimally run. This level is provided for information purposes only.

6.1.4.1.4 Dynamic Maximum Energy

Dynamic Maximum Energy specifies a level at or under which a Dynamic Schedule must run. This level is provided for information purposes only.

6.1.4.1.5 Current Level

Current level contains the level at which the transaction should be running based on all approved Requests processed in order of receipt by the Authority.

6.1.4.2 Profile Usage

The above-described profiles can be used in two different ways: as Base Profiles and as Exception Profiles

6.1.4.2.1 Base Profiles

Base Profiles describe the initially requested profile for implementation. At no time should there be more than one base profile of the same profile type in effect for the same point in time (i.e., it is invalid to have both a market level profile from 6-22 and 8-12 for the same provider). Note that it is acceptable for profile types associated with Dynamic Schedules to overlap (i.e., Dynamic Minimum 0MW from 6-22, Dynamic Maximum 100MW from 6-22, MarketLevel 80MW from 6-22).
Different types of transactions have different Base Profile requirements:

PROFILE TYPE	REQUIRED DATA FOR BASE PROFILE
GENERATION	MARKET LEVEL DYNAMIC MINIMUM ENERGY (for Dynamic Schedule Types) DYNAMIC MAXIMUM ENERGY (for Dynamic Schedule Types)
TRANSMISSION POR	MARKET LEVEL
TRANSMISSION POD	MARKET LEVEL
LOAD	MARKET LEVEL

The Authority will calculate the Base Current Level profile.
It is not valid for a Profile Change to contain a Base Profile.

6.1.4.2.2 Exception Profiles

Profile Modifications, or Exceptions, describe changes to the profile of the e-Tag that must be implemented in place of the original profile for a specified period of time. In all cases, the requested modification to the profile must go through an approval process. At no time should there be more than one exception profile of the same profile type in effect for the same point in time (i.e., it is invalid to have both a market level profile from Hours Ending 6-22 and Hours Ending 8-12 for the same provider). While it is possible to request an exception that overlaps a previous exception, the end result will be a single exception profile that covers the union of the prior exception and the new exception.
It is not valid for either a New e-Tag or a Correction to contain an Exception Profile.
The Services are responsible for determining the appropriate Current Level based on the profiles in their possession and generating the Current Level Profile.

6.1.4.2.2.1 Market Level Exceptions

A Market Level Exception defines the maximum level at which the e-Tag Author wishes the transaction to run if it differs from the original Market Level. This value is designed to allow the e-Tag Author to change the level of flow for a transaction, but continue to keep the capacity committed as originally specified. In so doing, the e-Tag Author reduces the need for detailed evaluation by Transmission Service Providers, as the originally requested transaction already specified appropriate transmission resources.

6.1.4.2.2.2 Reliability Limit Exceptions

The Reliability Limit defines the maximum level at which a Reliability Coordinator, Balancing Authority, or Transmission Service Provider wishes to run the transaction if it differs from the Market Level. This level is designed to change the level of flow for a transaction due to TLR events, USF, loss of generation, and loss of load.

6.1.5 Transmission Allocations

Transmission Allocations are a special kind of profile set that defines the way in which market participants will fill their capacity commitments with transmission reservations. Transmission Allocations specify a particular reservation, the provider associated with the reservation, and profiles associated with that reservation that describe how the reservation should be consumed. Transmission Allocations must always be associated with Transmission Physical Segments; association with other segments (such as Generation or Load) is not allowed. The Maximum Reservation Capacity associated with each physical segment should be greater than or equal to the energy profile. This is validated by the Tag Authority for new Tag creation requests only. Validation of subsequent adjustment Requests by the Authority is problematic due to sequencing and approval issues.

The transmission allocation for all transmission segments must be greater than or equal to the minimum of the POR profile and POD profile for that segment.

There are two types of profiles, both specified with Maximum Reservation Capacity profiles: Base Allocation Profiles, and Exception Allocation Profiles.

6.1.5.1 Base Allocation Profiles

Base Allocation Profiles define the original manner in which transmission reservations were allocated to meet capacity commitments. They are specified as a series of time-ordered segments of duration and the transmission capacity to be consumed. These segments may be repeated on multiple days, if so desired.

6.1.5.2 Exception Allocation Profiles

Exception Allocation Profiles define the manner in which transmission reservations are allocated to meet capacity commitments during changes to a Base Allocation Profile. They are specified as a series of time-ordered segments of duration and the transmission capacity to be consumed, and supersede data supplied in their corresponding base profile.

6.1.6 Loss Accounting

Loss Accounting data specifies the manner in which losses should be accounted for over a specified period of time. Over time, an e-Tag Author may elect to specify different choices for how losses will be provided. Each specification creates (or overwrites) Loss Method Entries, which are used to determine how losses are to be applied.

Section 7 - Messaging Overview

7.1 Messaging Concepts

7.1.1 Use of the Transmission Control Protocol/Internet Protocol

The services defined in this document utilize the public Internet as their physical communication layer. Therefore, the underlying root protocol for this specification shall be TCP/IP. Utilization of HTTPS based on NAESB PKI standard compliant certificates is expected to be phased in over time as infrastructure, such as the Electric Industry Registry, are available to support the implementation. Additionally, the services defined in this document shall send data via both Port 80 and 443, the common known port for HTTP and HTTPS respectively, using TCP connections. The use of HTTP or HTTPS will be based on the fully qualified URL. For HTTPS connections, a client certificate may be used. The recipient of an HTTPS connection must verify that the client certificate presented (if one is present) is valid for the sending entity.

When participating entities register for service, they will be required to supply information on the manner in which their implementation will address certain needs. Explicitly, they will need to define:
URL, Certificate Issuer, and Common Name for Authority Service (Balancing Authorities only)
URL(s) for Reliability Authority Forwarding (Balancing Authorities only)
URL, Certificate Issuer, and Common Name for Approval Service (Balancing Authorities, Transmission Service Providers, and optionally Purchasing Selling Entities)
URL, Certificate Issuer, and Common Name for Agents (Purchasing Selling Entities and optionally Balancing Authorities)
For the purposes of this document, a URL (Uniform Resource Locator) can be considered a two-part description of a resource. The first part describes the scheme used to communicate and the host the communication is to take place with:

http://www.nerc.com or https://www.nerc.com

The second part is the URI, or Uniform Resource Identifier. It describes a particular resource on a host:

/~gads/meetings.html

This distinction is important in that when implementing this Interface, the first portion of a URL will define the host to connect to, while the URI will define what resource to apply HTTP or HTTPS request to. Therefore, the following URL:

http://www.nerc.com/~gads/meetings.html

would be interpreted in the following manner:
<TCP/IP command> connect to “www.nerc.com”
<Application specific command> write the HTTP request to the connection
In the above example, the request would be “GET /~gads/meetings.html HTTP/1.1”

Both client and server certificates used for e-Tag communications must be compliant with NAESB PKI standards.

7.1.1.1 Establishing Connections

Establishing connections should be handled in the manner defined by the TCP/IP protocol.

For automated responses to queries, automated distributions, and other actions not specifically initiated by a person's action (CallbackHistory, CallbackSummaries, CallbackTags, DistributeCorrection, DistributeNewTag, DistributePotentialTLRProfileChange, DistributeResolution, DistributeProfileChange, DistributeStatus, RequestProfileChange*):

Should a connection attempt fail or any response other than a valid e-Tag Schema response be received, the service initiating the connection request must follow the procedures below prior to assuming the recipient's service is unavailable and indicating a message failure:

> At least three (3) attempts must be made to make the connection, with no less than five (5) seconds between each attempt, with the maximum time between the first and last attempts not to exceed two (2) minutes.

For actions specifically initiated by a person's action, such as Requests, Actions, and Queries (QueryHistory, QueryRequest, QueryRequestIDs, QueryStatus, QuerySummaries, QueryTag, QueryTags, RequestCorrection, RequestNewTag, RequestProfileChange*, SetState, WithdrawRequest):

Should a connection attempt fail or any response other than a valid e-Tag Schema response be received, the service initiating the connection request must assume the other service is unavailable and *immediately* indicate a message failure.

In both cases, message failures must alert the operator of the service attempting to send the message.

*If an automated system is issuing RequestProfileChange (i.e., an RAS), then the system *must* retry the connection. If the issuer is a person or operator, the system *must not* retry the correction, and instead alert the operator of the failure.

7.1.1.1.1 Partial Connection Failures

Should a connection attempt appear to fail between the Agent, Authority, and/or Approvals, yet messaging succeeded, an invalid set of errors may be encountered by re-sending the same message (i.e., e-Tag ID Not Unique errors), leading the sender to report incorrect error information. Should such a message duplication be attempted, the receiving service must respond back with a return State of DUPLICATE, and return any original additional response data back to the user (i.e., information other than that contained in the ReturnState data structure). This requirement does not apply to messages that it is valid to send multiple times such as query messages.

A message shall be considered a duplicate if

- The method called is the same as the previous message and,
- The entire MessageInfo data collection is the same as the previous message.

It should be noted that this behavior may only occur when messages are duplicates. For instances where a request is made and the information is *not* duplicated, the message must either be processed as a new message or marked as an error, depending on the specific situation (for example, submitting a new e-Tag with a previously submitted e-Tag ID is invalid, but submitting a new Profile Change must be processed normally).

7.1.1.1.2 Combining Messages

Previous versions of e-Tag allowed for the combining of messages in order to reduce messaging overhead. For Balancing Authorities, Transmission Service Providers, and Purchasing/Selling Entities, this functionality is no longer supported; for each specific entity, a distinct and separate message must be sent. For Reliability Coordinators, it is still allowed to send one message per unique forwarding URL.

7.1.2 Use the Hypertext Transport Protocol

e-Tag messaging is accomplished through the use of the Hypertext Transport Protocol (HTTP) over the public Internet, optionally using SSL (HTTPS). The e-Tag services defined in this document utilize HTTP 1.1.

7.1.2.1 HTTP/S Requests

The services defined in this document utilize a single HTTP method: the POST method. This method is used for sending data to a server for processing. The standard format of an HTTP Request Header is as follows:
<HTTP method> <resource URI> <HTTP Version>
In this implementation, all Request Headers will exist as the following:
POST <resource URI> HTTP/1.1
This specifies the POST method is to be used, the path and name of the processing resource, and that using HTTP 1.1 is the protocol and version being used. Additional header fields required are described below:
Content-type: text/xml

Declares that the type of data attached to the POST request will be an XML data set

Content-length: <integer>

Describes in bytes the length of the following attachment. The recipient utilizes this byte length to retrieve the Payload

SOAPAction:NERCETag18:<method name>

Indicates that the action being requested is part of the NERC e-Tag 1.8 library of methods, and specifies the method being called.

A Carriage Return/Line Feed terminates each header line. The request is completed by sending a Carriage Return/Line Feed on an empty line marking the end of the HTTP headers, followed by the Entity Data or Payload.

7.1.2.2 HTTP/S Responses

HTTP Responses are returned to a client with the following syntax:
<HTTP Version> <State Code> <Explanation>

The State codes below are utilized and understood by the TIS services defined in this document:

200	OK	States that the POST request was accepted and appears to be valid
400	Bad Request	States that the POST request was accepted but appears to point to an invalid URI or does not contain a valid Content-Type

Successful responses will be followed with an entity descriptor, describing the data to follow:

Content-type: text/xml

Declares that the type of data attached to the response will be an XML data set

Content-length: <integer>

Describes in bytes the length of the following attachment. The recipient uses this byte length to retrieve the Payload.

A Carriage Return/Line Feed terminates each response line. The response is completed by sending a Carriage Return/Line Feed on an empty line marking the end of the HTTP response, followed by the Entity Data or Payload. The payload for the purposes of this document shall be an e-Tagging Messaging Protocol message.

The server terminates the connection when the last of the payload has been transmitted.

7.1.3 How SMXP Works

All e-Tag 1.8 messages are sent using the SMXP (Simple Method Exchange Protocol). This protocol is based upon a *remote procedure call* paradigm. This means that instead of sending messages explicitly, you invoke procedures on remote machines, and pass any needed data as input parameters to the function. When the function is complete, it returns the result of its processing. The SMXP protocol is layered on top of the HTTP protocol, which handles all of the underlying communication. SMXP defines the set of rules for encoding remote procedure call parameters into HTTP POST messages, as well as the set of rules for how such messages must be processed by a remote server.

The steps of executing an SMXP method are as follows:

- A request is generated, containing the method name and any needed parameters.
- The request is sent via HTTP to a listener on the remote machine.
- The remote machine receives the SMXP request, and examines it to determine which method must be executed.
- The remote machine executes the appropriate method and packages the result into an SMXP compliant XML document.
- The remote machine returns that document to the calling machine (again via HTTP).

Each SMXP method call has two important parts – the request and the response. Most of the methods used in e-Tag 1.7 are *synchronous* methods, meaning that once the calling

machine makes a request, it waits for a response containing the results of its request before continuing.
In a few cases, *asynchronous* methods are used. In an asynchronous method, a request is generated and sent to a remote machine. The remote machine places the request into a queue, and sends a response to the calling machine that indicates the request has been received and queued for processing. The connection is then terminated. At some point in the future, the remote server runs the requested method and sends the result to the calling machine via a separate SMXP message (requiring a second request/response pair). Electronic e-Tagging systems are only required to support the processing of one method call per connection session. Multiple calls per session are not supported.

7.1.4 Method Types

E-Tag 1.7 uses various types of methods for various purposes. The methods can be broken up into the following categories.

7.1.4.1 Requests

A request method is any method that initiates an action associated with a transaction. Such actions include e-Tag submission and adjustment.

7.1.4.2 Request Distributions

Request Distributions are the methods used to send requests to the all entities impacted by the e-Tag. Request distributions may be informational, or may indicate a requirement for approval.

7.1.4.3 Actions

Actions are those methods that directly set a value. These methods include request approval, denial, and withdrawal.

7.1.4.4 Information Distributions

Informational distributions are the methods used to send information related to the State of a particular request or set of transactions. These are sent to entities to alert them of particular requests implementation or withdrawal, as well as specific entities approvals and denial of a request.

7.1.4.5 Queries

Query methods are used to search and recover data from an Authority or similar service. Most query methods use parameters that allow the server to filter unneeded data and return the smallest reply message possible. Which parameters may be specified depends upon which query method is called. Many queries are asynchronous methods, meaning the results of the query will return via a callback. Others are synchronous, meaning the response contains the results of the query. Queries may be sent more than once for the same data, however, Queries sent more than five times for the same data may be rejected.

7.1.4.6 Callbacks

Callbacks are methods that are used to return results from asynchronous queries. Each callback will be associated with a previously called query that was used to create the result set.

7.1.5 Faults

Fault messages are returned by any SMXP method that does not complete due to a structural error in the request. Such errors include any schema validation errors, such as incorrect data types and bad element ordering. Faults are also generated by message syntax errors, namespace errors, and some types of communication error. Fault messages indicate that processing was terminated before the requested procedure could be run. The SMXP specification defines the standard format and content for fault messages. Operators of the service attempting to send the message must be alerted to the receipt of any faults.

7.1.6 Return Values

Each method returns a State code that reports whether or not the method call was successful. A Return value of "SUCCESS" indicates that there were no errors in the method invocation, and that valid data was passed into the method. A value of "FAIL" indicates that that the method did not run successfully. If the State code is set to "FAIL", then an error message must be included which describes the error that was encountered. Operators of the service attempting to send the message must be alerted to the receipt of any FAIL returns.
In certain cases, the method may return a value of "DUPLICATE." This value indicates that the method being called has been previously called with identical parameters and a response has already been returned. Typically, this value is received after a partial connection failure and subsequent retry.

7.1.7 Error Messages

Error messages are generated whenever a method does not complete successfully due to problems with provided parameters or execution of the query (unless the problems have already been defined by a fault or HTTP error message). If an error message is present, the State code must have a value of "FAIL". Error messages indicate that the method was executed, but was unable to fulfill the caller's request due to problems encountered during the processing of the request. Error messages can be cause by passing invalid (but syntactically correct) data to a method or by internal system failures or outages.

7.2 Method Descriptions

The six fundamental method types align with the system concepts defined in Section 1 of this document. Those types are Requests, Request Distributions, Request Actions, Information Distributions, Queries, etc. Details about the exact composition of these various data elements are defined in the latest e-Tag schema .

7.2.1 Special Data Structures

Some methods require specific data structures. In cases where the structure is unique to a particular method, the structure will be defined with the method description.
Other generic structures are defined below.

7.2.1.1 Tag ID

Tag Ids are values that uniquely identify an e-Tag. It is composed of four values:

- The Source BA's NERC Acronym
- The Purchasing-Selling Entity's NERC Acronym
- A reference code assigned by the PSE to aid in identification of the transaction
- The Sink BA's NERC Acronym

The combination of these values must uniquely identify the e-Tag. At no point in time may two active e-Tags exist with the same e-Tag ID. To ensure this, an e-Tag ID may NOT be "reused" until a minimum of one (1) year has passed since the last point in time in which the e-Tag previously using the e-Tag ID ran.

7.2.1.2 Message Info

Message Info is a collection of data used to describe the basic communication characteristics of an e-Tag message. Message info is composed of four values:

- The NERC Acronym of the entity initiating the message transfer
- The Security Key used to ensure validity of the message
- The NERC Acronym of the entity to whom the message is being transferred
- A date and time indicating when the message was generated

This information must be used to identify message participants, as well as provide simple authentication and audit information.

7.2.1.3 Return State

Return State is a collection of data used to indicate the general results of a message being processed. Return State has three specific components:

- A date and time indicating when the return was generated
- A State of the processing
- Optionally, a list of errors encountered during the processing of the message

This information must be used to communicate semantic problems with a message back to a message initiator.
.

7.2.1.4 Miscellaneous Info

In many messages, it is possible to communicate token/value pairs of non-standard information. This is included as a convenience and method for extending the e-Tagging system. By using the Miscellaneous Info function, entities can pass along data to other parties that is not directly supported by the data model. For example, when initiating a curtailment request, an entity could provide various other information components, such as:
IMPACTED FLOWGATE : 1178
PROCEDURE : LLR

It is intended that entities make use of this feature in a standard, published manner that will allow recipients to process and utilize the information transferred.

7.2.2 Errors and Error Lists

The following are errors that may be supplied by the recipient of a method call should an error condition exist. The responder must provide an error number and a textual description of the error that provides specific detail about the error (i.e., information that will help the user resolve the problem). Supported errors are:

0001	Tag Already Exists	The e-Tag ID provided has already been used on an e-Tag held by the responding service.
0002	Tag Not Found	The e-Tag ID referenced is one not held by the responding service.
0003	Segment Not Found	The Segment referenced is not one held by the responding service
0004	Request Not Finalized	The profile cannot be changed, as it has not yet been finalized.
0005	Request Finalized	The e-Tag cannot be corrected or withdrawn, as it has already been finalized (CONFIRMED, IMPLEMENTED, etc.)
0006	Request Not Found	The referenced request is not one held by the responding service
0007	Stale Request	The request is inappropriate due to timing requirements.
0008	Invalid Range	The range specified exceeds or otherwise violates the rules associated with its definition
0009	Invalid Security Key	The security key provided is not correct
0010	Tag Not Requested	The e-Tag being presented is not one requested by the responding service
0011	Insufficient Rights	The requester does not have appropriate rights
0012	Contact Not Specified	A contact is required to be specified, and was not provided
0013	Reason Not Specified	A Reason is required to be specified, and was not provided
0014	Invalid Return Rate	The Return Rate was either not specified or incorrectly formatted
0015	Correction not allowed	The proposed correction would change the physical or financial path, which is not allowed.
0016	Missing Correction	The SetState request cannot complete because the Approver does not have the most recent correction for the segments in their scope.
0017	Missing DC Tie Operator	The RequestNewTag method cannot complete because a Balancing Authority registered to operate a requested DC Tie was not included as a Scheduling Entity for the Transmission

		Service Provider in the e-Tag.
0018	Orphan Profile	Every Profile must be reference by at least one Physical Segment
0019	Profile Not Found	The profile being referenced was not found in the e-Tag
0020	Invalid Path Order	The Market Segments, Physical Segments, and Parent market Segment References must be in correct order.
0021	Invalid Registered Value	A registered value is incorrect. This includes invalid or incorrect to/from entities, deactivated or unregistered PORs/PODs and/or Sources/Sinks, and non-existent products.

7.2.3 Initiating a Request

7.2.3.1 Special Data Structures

7.2.3.1.1 TimeClassification

Used to indicate to an e-Tag Author that a request was received on time, Late, or ATF based on the NERC/NAESB Standards timing guidelines.

7.2.3.2 Request New Tag

Issued by: Agents
Processed by: Authorities
Purpose: Used to submit a new e-Tag to the Authority for processing.

In	Message Info	Required
	Tag	Required
Out (successful)	Return State	
	Request ID	
	Late Flag	
Errors	0001Tag ID Already Exists	
	0007 Stale Request	
	0017 Missing DC Tie Operator	
	0018 Orphan Profile	
	0020 Invalid Path Order	
	0021 Invalid Registered Value	

7.2.3.3 Request Correction

Issued by: Agents
Processed by: Authorities
Purpose: Used to submit changes to a new e-Tag while it is being evaluated for approval

In	Message Info	Required

	ContactInfo	Required
	Tag ID	Required
	Correction List	Required
	Notes	Optional
Out (successful)	Return State	
	Correction ID Set	
Errors	0002 e-Tag ID Not Found	
	0003 Segment Not Found	
	0005 Request already in Final state	
	0009 Invalid Security Key	
	0015 Correction Not Allowed	
	0021 Invalid Registered Value	

7.2.3.4 Request Profile Change

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to change the energy level or transmission allocation associated with a particular e-Tag.

In	Message Info	Required
	Contact Info	Required
	Tag ID	Required
	Market Profile Change OR Reliability Profile Change	Required
	Miscellaneous Info List	Optional
	Notes	Optional
Out (successful)	Return State	
	Request ID	
	Late Flag	
Errors	0002 e-Tag not found	
	0007 Stale Request	
	0009 Invalid Security Key	
	0011 Insufficient Rights	
	0012 Contact not Specified	
	0013 Reason not Specified	
	0019 Profile Not Found	
	0021 Invalid Registered Value	

7.2.4 Request Distribution

7.2.4.1 Special Data Structures

7.2.4.1.1 Approval Rights Flag

Used to indicate that a recipient of a request distribution has approval rights over the request.

7.2.4.1.2 Impact Flag

Used to indicate that a recipient of a correction request distribution has a need to re-evaluate the e-Tag based on the correction.

7.2.4.2 Distribute New e-Tag

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to distribute new e-Tag requests to parties with rights to view or approve the request.

In	Message Info	Required
	Tag	Required
	Approval Rights	Required
	Late	Optional
Out (successful)	Return State	
Errors	0001 e-Tag already exists	
	0021 Invalid Registered Value	

7.2.4.3 Distribute Correction

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to distribute a correction to parties with rights to view or approve the original new e-Tag request.

In	Message Info	Required
	Contact Info	Required
	Tag ID	Required
	Correction List	Optional
	Loss Accounting List	Optional
	Impact Flag	Required
	Late Flag	Required
	Notes	Optional
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0003 Segment Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.4.4 Distribute Profile Change

Issued by: Authorities

Processed by: Agents, Approvals, RASs
Purpose: Used to distribute a request to change a profile to the parties with rights to view or approve the original new e-Tag request.

In	Message Info	Required
	Contact info	Required
	Tag ID	Required
	Approval Rights	Required
	Request ID	Required
	Requestor	Required
	Late	Required
	Exception Profile Change	Optional
	Transmission Allocation Change List	Optional
	Loss Accounting Change List	Optional
	Misc Info list	Optional
	Notes	Optional
	Request Time Stamp	Required
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.5 Request Actions

7.2.5.1 Set State

Issued by: Approvals
Processed by: Authorities
Purpose: Used by entities with Approval Rights to a request to specify their commitment to implement or reject the request.

In	Message Info	Required
	Tag ID	Required
	Scope	Required
	Request Ref	Required
	Approval Status	Required
	Approval Time Stamp	
	Notes	Optional*
Out (successful)	ReturnState	
Errors	0002 e-Tag Not Found	
	0003 Segment not Found	
	0005 Request Finalized	
	0009 Invalid Security Key	
	0013 Reason not Specified	
	0016 Missing Correction	

	0021 Invalid Registered Value

*Required for states of Denied or Study.

7.2.5.2 Withdraw Request

Issued by: Agents, Approvals, and RASs
Processed by: Authorities
Purpose: Used by request authors to remove their request from consideration prior to the completion of its evaluation.

In	Message Info	Required
	Contact Info	Required
	Tag ID	Required
	Request Ref	Required
	Notes	Optional
Out (successful)	Return State	
Errors	0002 e-Tag not found	
	0005 Request Finalized	
	0006 Request not found	
	0009 Invalid Security Key	
	0011 Insufficient Rights	
	0012 Contact not specified	
	0021 Invalid Registered Value	

7.2.5.3 Terminate Request

Issued by: Agents, Approvals
Processed by: Authorities
Purpose: Used by request authors to set the transmission and energy profiles of an e-Tag to zero and set its state to TERMINATED after the request has transitioned to IMPLEMENTED.

In	Message Info	Required
	Contact Info	Required
	Tag ID	Required
	Request Ref	Required
	DateTime	Required
	Notes	Optional
Out (successful)	Return State	
Errors	0002 e-Tag not found	
	0005 Request Finalized	
	0006 Request not found	
	0007 Stale Request	
	0009 Invalid Security Key	
	0011 Insufficient Rights	
	0012 Contact not specified	

	0021 Invalid Registered Value

7.2.6 Information Distribution

7.2.6.1 Distribute Status

Issued by: Authorities
Processed by: Agents, Approvals, and RASs
Purpose: Used to notify entities with Approval and Viewing rights of other Approver's actions with regard to a particular request.

In	Message Info	Required
	Tag ID	Required
	Request Ref	Required
	Status List	Required
	Flowgate List	Optional*
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0006 Request not found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.6.2 Distribute Resolution

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to notify entities with Approval and Viewing rights of the final resolution of a particular request.

In	Message Info	Required
	Tag ID	Required
	Request ID	Required
	Request Status	Required
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0006 Request not found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.6.3 Distribute Potential TLR Profile Change

Issued by: RASs
Processed by: Agents
Purpose: Used to inform e-Tag Authors about potential impending profile changes due to TLR.

In	Message Info	Required

	Start Date Time	Required
	TLR Event Ref	Required
	Misc Info list	Optional
	TLR Profile Change List	Required
Out (successful)	Return State	
Errors	0021 Invalid Registered Value	

7.2.6.4 Callback Potential TLR Profile Change

Issued by: Agents
Processed by: RASs

In	Message Info	Required
Out (successful)	Return State	
Errors	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7 Query Functions

7.2.7.1 Query Summaries

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to request a list of e-Tags and keys based on search criteria. Primarily used for recovery purposes.

In	Message Info	Required
	Range	Required
Out (successful)	Request ID	
Errors	0008 Invalid Range	
	0021 Invalid Registered Value	

7.2.7.2 Callback Summaries

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to send a list of e-Tags and keys to an entity that has previously requested via QuerySummaries.

In	Message Info	Required
	Tag Summary List OR Empty Element	Required
Out (successful)	Return State	
Errors	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.3 Query e-Tag

Issued by: Agents, Approvals, and RASs
Processed by: Authorities
Purpose: Used to retrieve a single e-Tag from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag ID	Required
Out (successful)	Return State	
	Tag	
Errors	0002 e-Tag not found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.4 Query e-Tags

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to request multiple e-Tags from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag Credential List	Required
	Return Rate	Required
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0014 Invalid Return Rate	
	0021 Invalid Registered Value	

7.2.7.5 Callback e-Tags

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to send multiple e-Tags from an Authority to an entity that requested them via QueryTags. Primarily used for recovery purposes.

In	Message Info	Required
	Tag List OR Empty Element	Required
Out (successful)	Return State	
Errors	0009 Invalid Security Key	
	0010 e-Tag Not Requested	
	0021 Invalid Registered Value	

7.2.7.6 Query History

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to retrieve a single e-Tag's History from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag ID	Required
Out (successful)	Return State	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.7 Callback History

Issued by: Authorities
Processed by: Agents, Approvals, RASs
Purpose: Used to send a single e-Tag's History from an Authority to an entity that requested it via QueryHistory. Primarily used for recovery purposes.

In	Message Info	Required
	History	Required
Out (successful)	Return State	
Errors	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.8 Query Request

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to retrieve a specific request for a single from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag ID	Required
	Request ID	Required
Out (successful)	Return State	
	RequestProfileChange	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.9 Query Request IDs

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to retrieve a list of requests made regarding a single e-Tag from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag ID	Required
	Request Status(es)	Optional
Out (successful)	Return State	
	Request ID Summary List	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.10 Query Status

Issued by: Agents, Approvals, RASs
Processed by: Authorities
Purpose: Used to retrieve a request's State from an Authority. Primarily used for recovery purposes.

In	Message Info	Required
	Tag ID	Required
	Request Ref	Required
Out (successful)	Return State	
	Request State	
	Approver State List	
Errors	0002 e-Tag Not Found	
	0009 Invalid Security Key	
	0021 Invalid Registered Value	

7.2.7.11 QueryAvailability

Issued by: Agents, Approvals
Processed by: Agents, Approvals, and Authorities
Purpose: Used to determine availability/status of an e-Tagging service. Primarily used to evaluate system performance.

In	From Entity	Required
	To Entity	Required
Out (successful)	Return Time Stamp	
	Request Value	

Errors	0021 Invalid Registered Value

Specification for Implementation of Conditional Firm in e-Tagging

Overview

This document describes how the NAESB Electronic Scheduling Subcommittee/Information Technology Subcommittee (ESS/ITS), NERC/NAESB Joint Interchange Scheduling Working Group (JISWG), and e-Tag vendors determined that e-Tagging should be modified and utilized in order to support FERC Order 890 conditional firm implementation by the electric industry. This document does not include modifications to OASIS that will be necessary to support conditional firm. This document is being posted for comment so that industry participants may provide JISWG and ESS/ITS with input prior to JISWG modifying the e-Tag specifications and schema for conditional firm implementation.

Business Considerations

The ESS/ITS and JISWG considered the following "attributes" of long-term "conditional firm" (i.e., conditional curtailment options) service in its design specifications for e-Tagging:

- Conditional firm service, during the pre-defined conditions as identified in the System impact Study and included in the Service Agreement, will be treated on par with network transmission service from non-designated resources, i.e., priority 6 – higher than non-firm point-to-point service and lower than firm service.
    - The specific conditions whereby conditional firm service may subject to curtailment at priority 6 are beyond the scope of the JISWG. This specification is limited only to how the JISWG envisions communicating the change in service priority should such conditions arise.

Predefined system conditions require that the Transmission Service Provider (TSP) have the ability to:

- force a previously firm (priority 7) transaction to be treated on par with network service from non-designated resources
- override the PSEs submission of a priority 7 transaction to priority 6
- raise a previously limited transaction back to firm priority
- override and "split" the transaction into a firm and non-firm allocations

Design Considerations

In order to expedite this feature coincident with e-Tag 1.8 implementation, existing e-Tag schema and methods were used and the design was kept as simple as possible. The TSP may make unilateral (no approval process) changes to product code and transmission allocation(s) (including adding or deleting stacked allocations) for any segments where they are listed as the TSP as long as the total transmission allocation remains the same The TSP may make no other unilateral changes.

Specification

While a tag creation request is still pending, a Transmission Service Provider will be allowed to issue a correction to a transmission segment where they are the listed TSP. This will allow the TSP to change the priority of service in cases where the tag was using conditional firm service at priority 7 and it now needs to be used at priority 6 (or vice versa). Once the tag is implemented, a Transmission Service Provider will be allowed to issue an adjustment request that will accomplish the same goal, changing some or all of the conditional firm service being used at priority 7 to priority 6 (or vice versa).

The ability to issue a correction will differ from current practice in the following ways.

1. The correction will be issued by a TSP, rather than the tag author PSE.
2. The correction will only be allowed to affect transmission segments where the TSP sending the correction is the TSP of the segment.
3. The correction can only change the product code and transmission allocation(s). No other fields may be modified.
4. No approvals are required for TSP corrections of this type and the time characteristics of the e-Tag remain the same (i.e. ActOnByTime and TimeClassification).

The ability to issue an adjustment will differ from current practice in the following ways.

1. This will be a market adjustment issued by a TSP.
2. The adjustment may not change any energy profiles or any fields except for the product code and transmission allocation.
3. The adjustment may only modify or add transmission allocations associated with a transmission segment where the TSP sending the correction is the TSP of the segment.
4. The total transmission allocation for the physical segment must be the same before and after the change.
5. The adjustment cannot affect any profiles in the past. Changes may only be made from the time the request message is received by the Authority service forward.
6. The adjustment will be automatically approved and distributed by the Authority service as soon as it is received by the Authority service.

In practice, when conditions arise that require the firm service to be treated as non-firm service, the TSP will adjust an implemented tag by issuing a market adjustment that reduces the MW level of existing priority-7 allocation by the amount of conditional firm that is subject to change, and add/modify priority-6 allocations for the amount by which the existing firm allocation was reduced. When the conditions cease to exist, the TSP will adjust the tag by increasing the firm allocation and decreasing the non-firm allocation by the same amounts.

Additional Information

The above design would allow TSPs to create vertically stacked transmission allocations where one allocation would have a product code of 6-NN for example and another allocation on the same physical segment would have a product code of 7-F. The more typical case would be to adjust the 7-F allocation to zero for a specific time range and add an exception block for the same time range set to the original allocation with a 6-NN product code.

The above design requires the transmission level to be left unchanged since there is no approval process. If the energy level needs to be capped due to a decrease in available transmission capacity, then it is more appropriate for the TSP to issue a reliability adjustment.

By allowing corrections and adjustments, the TSP is allowed to change the product code associated with the physical segment without needing to issue exception profiles.

This design is silent on user interface features. Industry participants should work with their vendors on user interface functionality, particularly the interaction between OASIS nodes and e-Tagging systems.

The conditional firm support described above is scheduled for release with 1.8 implementation in early December 2007.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC/NAESB e-Tag 1.8 FAQ

1. What are the criteria for the "CC" field?
   e-Tag 1.8 provides this capability, but does not specify its use. "Criteria" would be part of NAESB business practice standards, NERC reliability standards, and/or regional business practices. The purpose of the CC field is to provide notification (copy of the e-Tag) to parties who are not in the physical or market path. This is useful for scheduling jointly owned units, etc. Entities who are in the physical or market path may not also appear in the CC list. Entities in the CC list have no approval rights.

2. Who designates/requests entities that will be placed on the "CC" list?
   The tag author is the only tagging entity that can populate the carbon copy list. Any other entity may request that they or some other entity be placed in the list according to applicable business practices, standards, contractual requirements, etc.

3. If entries are made to the e-Tag 1.8 incorrectly, will the author be notified with some sort of text message?
   Tag authors are informed of errors through three mechanisms – the agent has certain required validation checks and possibly has other optional validation checks provided by the vendor. Violation of either of these validation checks is presented to the tag author through the vendor's graphical user interface (GUI).

   The authority service also performs certain required basic validation checks and will return an error message to the agent service. The display of the error message contents is vendor specific.

   Lastly, approval entities to the tag may in their assessment discover errors and will deny the tag with a meaningful reason. The denial reason field is returned from the approval service to the author and distributed to all entities on the tag. Again, display of denial reasons is vendor specific.

4. How will the mechanics work on the December 4 or 5 switch-over? Will the User's PC have to be turned off (rebooted)? What are the details for the cut-over plan?

   To a certain degree, the transition from 1.7097 to 1.8 is vendor specific. In general, the vendors and JISWG have developed the following:
   - December 4, 2007 target date
   - Tags with TP in the SE field past the cutoff date/time are terminated at the cutoff date/time.
   - 21:30 to 22:00 CST quiet time
   - All pending requests set to Dead
   - All active 1.7097 tags ported to 1.8

- Users probably log-out, log-back-in
- 22:00 CST 1.8

Please coordinate with your vendor for exact instructions.

5. Who has the final say in performing the cut-over plan? Do the industry participants have the authority to say "no-go" or "are good to go"? Do we need to perform an individual user approval process?
   The JISWG requests that any entity that believes they will be unable to affect the planned 1.8 transition on or about December 4, 2007, to please notify JISWG, NERC, NAESB, their regional council, FERC, the Office of Homeland Security, and your local search and rescue organizations. The JISWG will post periodical updates of each deficient entity's progress and send reports to FERC.

6. Will the tagging templates roll over to e-Tag 1.8?
   Please contact your vendor for details. All vendors have been given a transition cross reference for active tag migration.

7. Will delaying the cut-over to 1.8 on Dec 4 or 5 cause any side effects?
   If any entity delays the cut-over and the rest of the industry cuts over to 1.8 then you will be unable to participate in tagging. In addition, you may be in violation of NAESB and NERC standards. Should these side effects last over 4 hours, please see your compliance officer. If the entire industry delays cutting over to 1.8 on Dec 4th, then the benefits provided by 1.8 will be delayed as well.

8. What is the impact of the 1.8 e-Tag changes?
   In general, there should be limited need to change downstream applications. On January 3, 2007, e-Tag 1.7097 was rolled into production to provide a minimum level of compliance with the new NERC INT standards. Several of the 1.8 features further that goal of providing an effective tool for interchange compliance, as well as provide certain capabilities associate with Order 890. Additional 1.8 modifications remove previous limitations in the tool. These modifications are not necessarily required to implemented, but are there to facilitate current and future business practices.

   The "impact" of the changes will vary from entity to entity depending on their vendor, architecture, downstream utilization of various fields and structures, etc. Each entity will need to assess and answer that question.

9. Regarding the tag correction process, the tutorial refers to the "network" transmission service and product codes. Please explain that slide? Who are impacted entities?
   During 1.8 development, it was brought to JISWG's attention that there are situations where a denying approval entity would not be considered an impacted entity for corrections to that denial. Specifically, Order 890 reemphasized the need for firm energy and transmission to support designated network resources. Typically, a tag representing the energy flow from a designation network resource to network load shows the network transmission service provider listed as the last transmission segment or sink segment. This tag may be denied by the network transmission service provider because one or more products (either energy or transmission) listed in the tag are non-firm. Typically, these products are listed in the generation or first transmission segments. Corrections to the first part of the physical path under 1.7097 did not include the last TSP, BA or LSE as

impacted entities. It is the impacted entities that are required to reassess the tag after a correction. E-Tag 1.8 now defines (in addition to the existing impacted entities) the last TSP, BA, and LSE in the physical path as impacted entities.

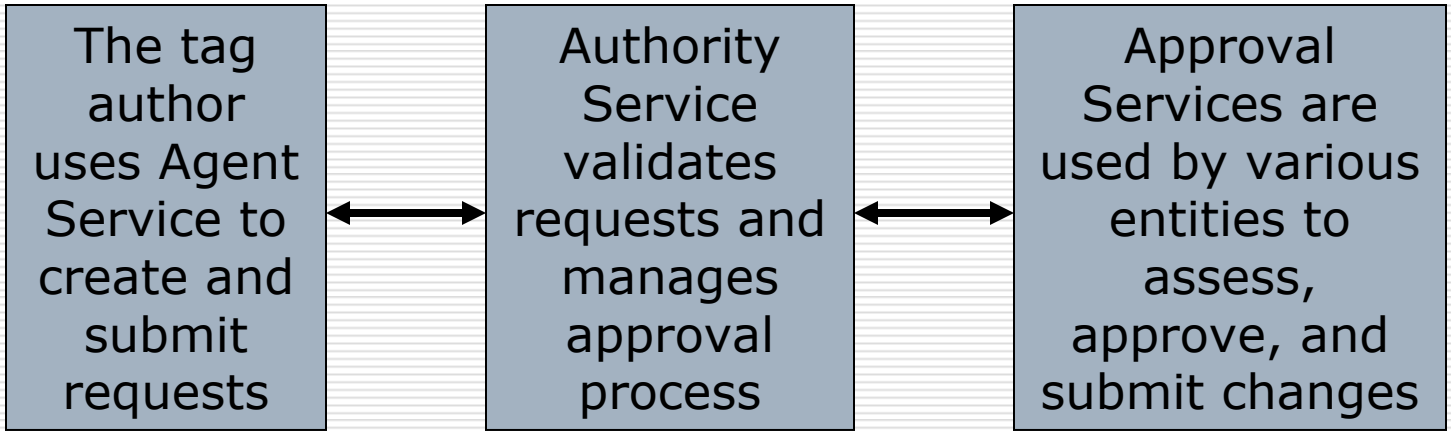
10. Will the practice of using a "TSP" code in the SE field remain in 1.8, or do we need to put the "TSP" code in the carbon copy field?
    Only BAs can listed in the SE field under 1.8. Any other entities that need to receive a copy of a tag must be entered into the carbon copy list. The NERC definition of Scheduling Entity is the entity implementing the transaction. The NERC standards define the BA as performing the function of transaction implementation. Additionally, NERC standards require that the BA across which the power is flowing for a physical segment be notified. Additionally, TP and BA codes frequently match, even though they are different entities. Restricting the use of the SE field to BA will help prevent this error.

e-Tag 1.8

An industry tutorial

e-Tag 1.8

- The basics features of e-Tag 1.8 are much the same as in the current 1.7097 version



e-Tag 1.8

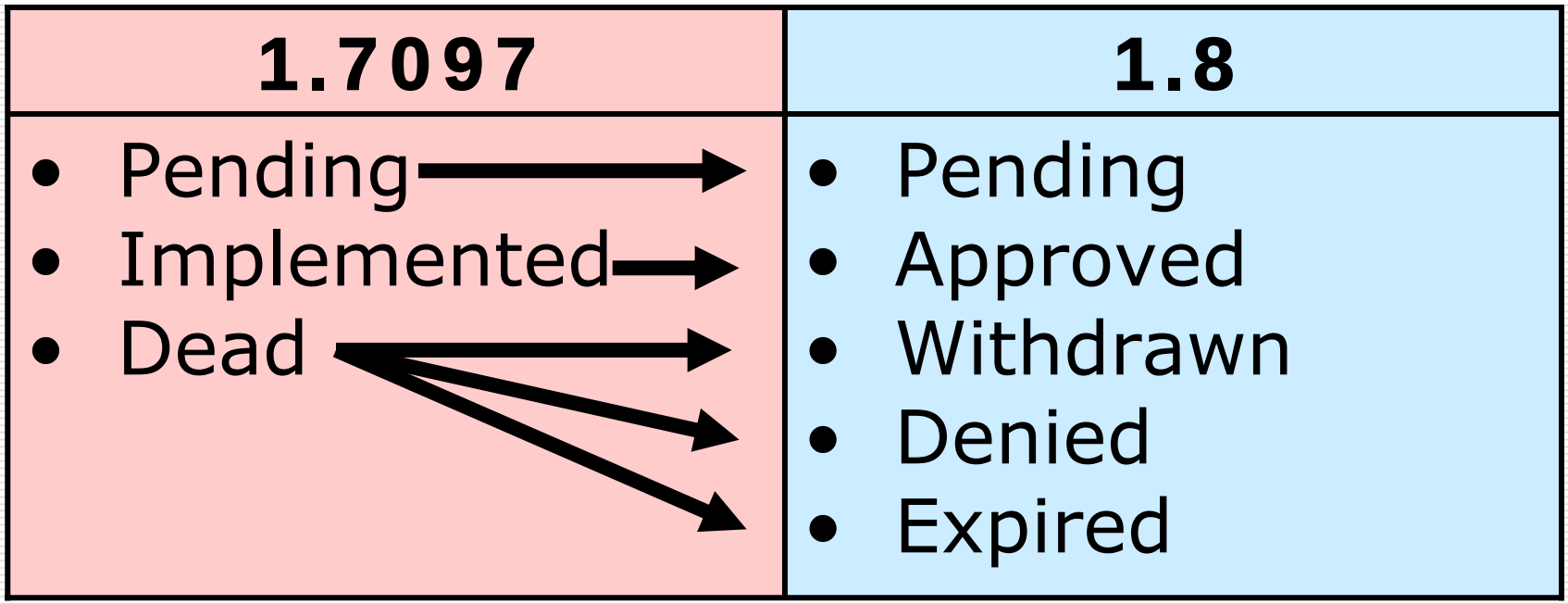
- "Requests" are a basic of e-Tag
- There are "new tag" requests – the initial submittal of a Request for Interchange. Once fully approved, it becomes the e-Tag.
- There are "change" or "adjustment" requests – a market adjustment and a reliability curtailment are two examples of change requests

e-Tag 1.8

- There are “correction” requests which can be made while the overall state is still “PENDING”
- Requests have status assigned by the authority service to describe their overall state
- The e-Tag is a collection of one or more associated Requests

e-Tag 1.8

- Request states



e-Tag 1.8

- Almost every request requires assessment and response from approval entities
- Each approval entity's response is assigned an approval state

e-Tag 1.8

- Individual Approval States

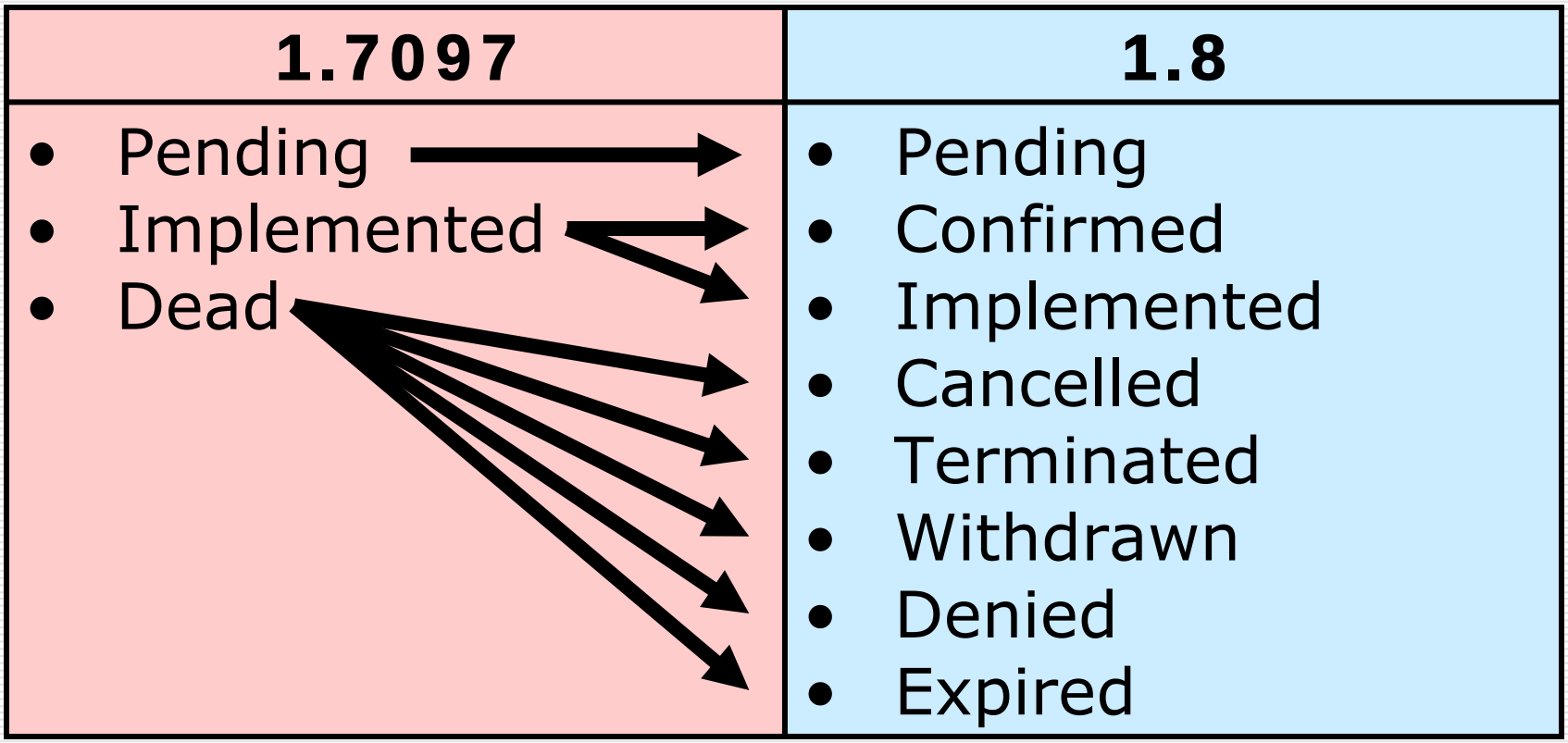
1.7097	1.8
• NA • Pending • Approved • Denied • Study	• NA • Pending • Approved • Denied • Study • Expired

e-Tag 1.8

- The composite state indicates the overall state of the e-Tag

e-Tag 1.8

- Composite States



e-Tag 1.8

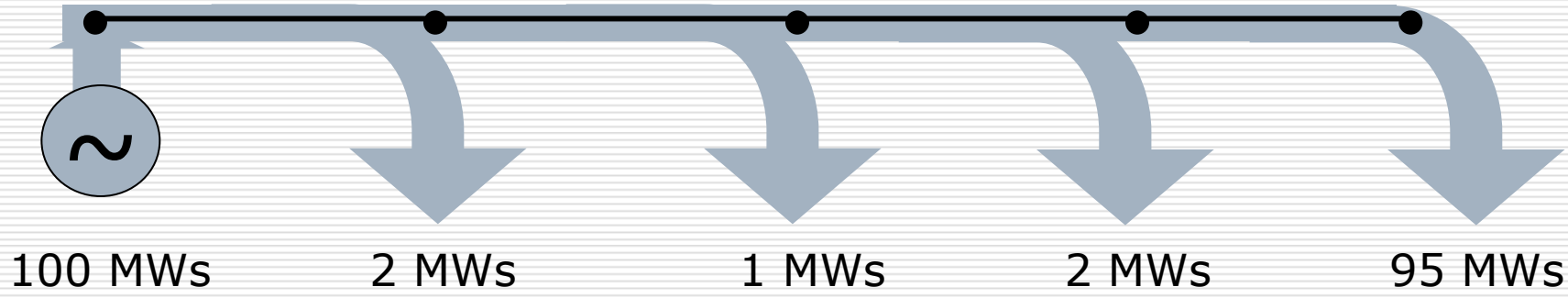
- Formalization of the Time Classification schema element
- Authority Service assigns based on the relative ramp start and submittal time
  - On-time
  - LATE
  - ATF

e-Tag 1.8

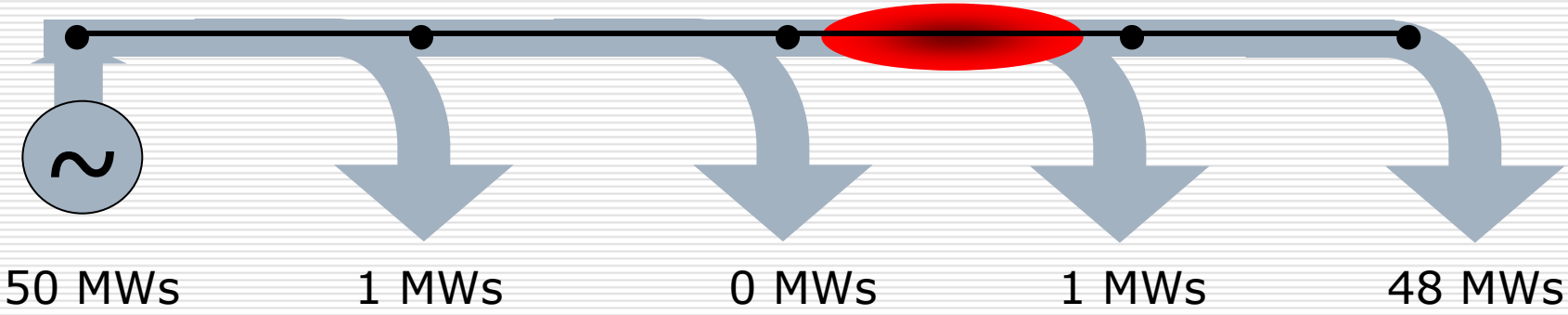
- Improved loss calculations for reliability curtailments, only
- In 1.7097 the Authority Service recalculated in-kind losses for a curtailment from the source BA to the sink BA, regardless of the curtailed segment
- In 1.8 the curtailing entity will specify the segment with the restriction and the Authority Service will recalculate losses both up-stream and down stream of that segment

e-Tag 1.8

- In 1.7097…

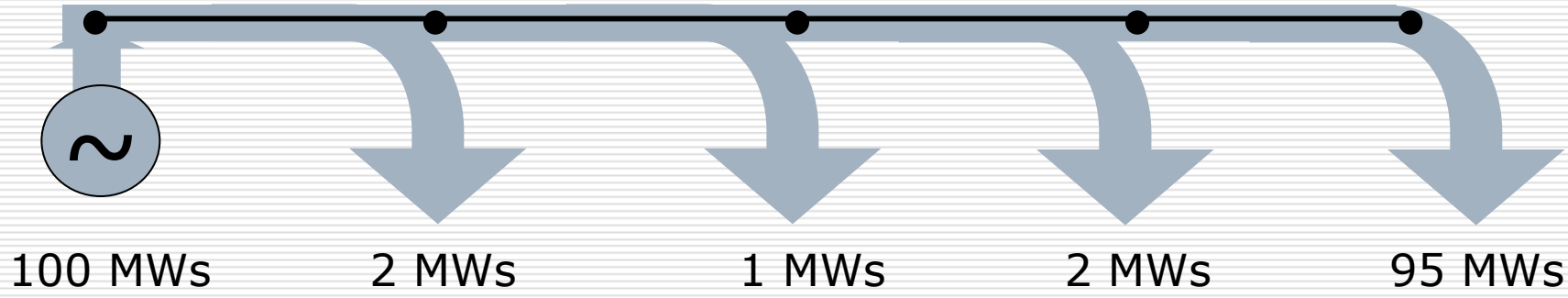


Third segment has a 50 MW restriction, Authority recalculates:

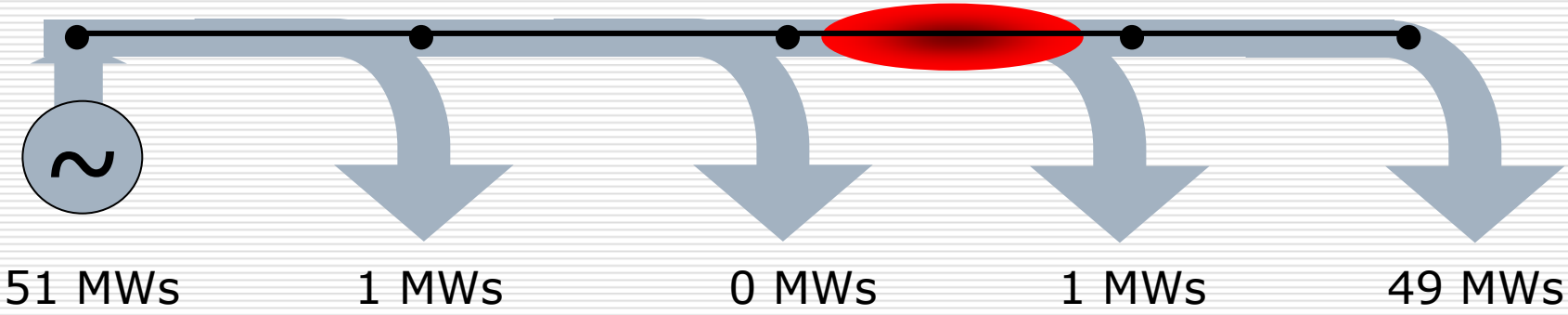


e-Tag 1.8

- In 1.8…



Third segment has a 50 MW restriction, Authority recalculates:



e-Tag 1.8

Carbon Copy Field

- In 1.8 the Tag Author may specify other BAs, TSPs, or PSEs who need to know about the transaction but who are not listed in either the market or physical paths in the e-Tag.
- Carbon Copy entities do not have approval rights

e-Tag 1.8

Conditional Firm

- The Order 890 pro forma tariff contains an option for long-term point-to-point service, sometimes referred to as conditional firm
- When dictated by the Transmission Service Provider's service agreement and business practices, service receiving this option can be changed from 7-F to a 6-NN and back again
- e-Tag 1.8 enables a TSP to change the product code and transmission profile(s) (as long as total is the same) associated with any transmission segment on the tag that references that TSP

e-Tag 1.8

Corrections to Products

- In e-Tag, while a request is still pending, the tag author can make corrections to certain information
- Any correction requires the re-assessment of the tag by impacted entities
- The e-Tag specification defines who the impacted entities are based on the information being changed
- Order 890 requires firm network transactions to be firm energy on firm transmission
- The last TSP or sink BA may deny the tag if non-firm energy and/or transmission product codes are used
- For product code corrections, 1.8 will include the last TSP, sink BA, and LSE in the impacted entity list

e-Tag 1.8

Corrections to Products (con't.)

- In 1.7097, impacted entities were defined as:

Correction Type	Impacted Entity
Any allowable correction to a Physical Generation Segment	Source BA, Generation Providing Entity
Any allowable correction to a Physical Transmission Segment or Transmission Allocation	Transmission Service Provider, Scheduling Entities (Intermediate BAs), Transmission Customer
Any allowable correction to a Physical Load Segment	Sink BA, Load Serving Entity
Any allowable correction to a Market Segment	Purchasing-Selling Entity

e-Tag 1.8

Corrections to Products (con't.)

- In 1.8, impacted entities are defined as:

Correction Type	Impacted Entity
Any allowable correction to a Physical Generation Segment	Source BA, Generation Providing Entity
Any allowable correction to a Physical Transmission Segment or Transmission Allocation	Transmission Service Provider, Scheduling Entities (Intermediate BAs), Transmission Customer
Any allowable correction to a Physical Load Segment	Sink BA, Load Serving Entity
Any allowable correction to a Market Segment	Purchasing-Selling Entity
Any allowable correction to any product code (energy or transmission)	**In addition to the above, the last Physical Transmission Segment's TSP, LSE, Sink BA**

e-Tag 1.8

Energy and Transmission Profiles

- The Agent and Authority Services will require the e-Tag's transmission allocation profile to be **≥** the energy profile

e-Tag 1.8

ATF Tags

- In 1.7097, ATF e-Tags could not be Terminated if a mistake was made
- In 1.8 an ATF e-Tag can be Terminated

e-Tag 1.8

ATF Tags

- In 1.7097, ATF e-Tags are restricted to a duration of one hour and can be submitted up to 48 hours in the past.
- In 1.8, ATF e-Tags are still restricted to a duration of one hour but may now be submitted with a start time up to 168 hours in the past.

e-Tag 1.8

Dynamic Adjustments

- In e-Tag 1.7097 only the e-Tag author could submit energy profile adjustments to a Dynamic type e-Tag
- e-Tag 1.8 will allow the Source and Sink BAs to also submit energy profile adjustments to Dynamic type e-Tags

e-Tag 1.8

Dynamic Adjustments

- In 1.7097, adjustments to DYNAMIC e-Tags are limited to 96 hours in the past
- In 1.8, DYNAMIC e-Tags may be adjusted up to 168 hours in the past, i.e. the actual hour being adjusted may not be more than 168 hours in the past.

e-Tag 1.8

New Transaction Type "Pseudo Tie"

- Within the context of e-Tag 1.8, this type behaves exactly like Dynamic transaction type (it is just a different label for unique identification purposes).
- Systems using e-Tags may need modification to properly account for the Pseudo Tie transaction type.

e-Tag 1.8

Scheduling Entity Field

- In the WECC, 1.8 requires a single Scheduling Entity (BA) in each transmission segment
- All other interconnections it is not required to be specified by the tag author if the Scheduling Entity code for the physical segment is identical to the Transmission Service Provider (TSP) code on that physical segment.

e-Tag 1.8

Ramping

- Ramp Rate is replaced with Ramp Duration
- Users will no longer see a ramp duration on intermediate interchange scheduled blocks
- CI Standards specify default ramp start and ramp stop times
- Uses a default ramp duration of zero for reliability “curtailments”, but will allow the user to specify a non-zero duration
- Uses separate default straddle ramps for Western and Eastern Interconnections.

e-Tag 1.8

Rounding Standard

- Within e-Tag 1.8, a rounding standard to move MW values the nearest whole MW was added to be used in loss calculations. MW values in e-Tag profiles are sometimes integrated into MWh values across schedule intervals. e-Tag profiles that start or stop within schedule intervals may result in fractional MWh values being calculated.
- (< .50 down, >= .50 up).

e-Tag 1.8

Improved Recovery Function

- Recovery is a mechanism that an Agent or Approval Service can request all updates from all Authority Services for any missed requests
- Vendor displays may vary – user initiated recovery not always available

e-Tag 1.8

Communications Security

- Added SSL via HTTPS and client certificate requirement based on NAESB PKI standard.
- Initial roll-out will require server-side only
- Client-side implementation will be phased-in over time
- Companies will need to work with their specific vendor as implementation requirements will vary.

e-Tag 1.8

The Rollout Schedule

- Remote Interoperability Vendor Testing with NERC/NAESB facilitation was successfully performed in August
- Sept. 7 through Nov. 2, 2007, User Training and Testing - industry participants and vendors may use this time to train their users and modify their back-office software, as necessary, for 1.8 changes

e-Tag 1.8

The Rollout Schedule (con't.)

- September 7, 11, and 25, 2007 Industry Tutorial/Q&A/Information Sharing through three 2-hour conference calls/webcasts
- Oct 22 & 29, 2007 unstructured testing for conditional firm implementation
- Nov 5-9 Final Interoperability Testing

e-Tag 1.8

The Rollout Schedule (con't.)

- **December 4, 2007 e-Tag 1.8 target Implementation**
- Project is on schedule and 12/4 is cutover date unless a Vendor or participant is not ready. In that case, the other vendors and participants would then be told which vendor or participant and why, along with new target date.

e-Tag 1.8

The Transition from 1.7097 to 1.8

- December 4, 2007 target date
- 21:30 to 22:00 CST quiet time
- All pending requests set to Dead
- All active 1.7097 tags ported to 1.8
- Users probably log-out, log-back-in
- 22:00 CST 1.8 – it's, it's ALIVE
- And cannot be killed

e-Tag 1.8

- Capabilities versus Requirements
- e-Tag 1.8 contains new features and capabilities such as the new Pseudo-Tie transaction type, Carbon Copy list, after-the-fact adjustments to DYNAMIC by BAs, conditional firm changes, etc.
- The presence of these new features and capabilities does not require industry participants to utilize them beyond applicable standards

Questions?

FIN

Cutover plan

The cutover should occur on a Tuesday or Wednesday. The plan assumes that the cutover will be on Tuesday, December 4, 2007. All times listed are in central prevailing time. Each vendor will provide contact info (phone and email) that other vendors can use immediately before/after the cutover to resolve any last minute problems.

21:30	Tag authority services stop accepting new requests. Tag authority services should return a fault message for any new request message received after this time (RequestNewTag, RequestCorrection, SetApprovalState, RequestProfileChange). All non-request messages (distribute and query messages) will be sent/processed normally.
21:30 – 21:45	Tag authority services resolve all pending requests to a state of "Dead", listing all approval parties that have not taken any action as passively denied. Send out all of the usual messages to approval parties, etc. to indicate resolution. All messages for all tags should be COMPLETE before 22:00. Any e-Tag terminations required by procedures below should be terminated during this period.
21:45 – 22:00	Port all 1.7 tags to 1.8 format tags using the procedure described below
22:00	E-Tag 1.8 goes live!!!

Procedure for porting e-tag 1.7 tags to e-tag 1.8

Terminate all active tags containing data that can't be sent via e-tag 1.8 XML messages. Tags meeting this criteria are:

1. Any tag that includes a scheduling entity of type TP

To terminate the tag, the tag authority will issue a PSE adjustment for the tag (listing the tag author as the request author) that sets the energy and transmission profiles to zero from 22:00 until the end of the tag. The tag authority will not accept new requests on such tags (even after the cutover). The PSE adjustments will be distributed normally, and will be automatically approved by the tag authority (approval status type will be set to "override" for all approval parties).

Create the 1.8 request state for all existing requests using this mapping:

1.8 Request state	1.7 Request state
Approved	Implemented
Denied	Dead/Pending (there should not be any pending requests at this point)

Create the 1.8 tag state using this mapping:

1.8 Tag State	Tags mapped to state

Confirmed	All tags where the tag creation request is implemented and the tag start time is in the future
Implemented	All tags where the tag creation request is implemented and the tag start time is in the present/past
Denied	All tags that have 1.7 request state of “dead” for the tag creation request, regardless of why that request went to “dead”.
Pending	There should be no tags mapped to this state
Withdrawn	There should be no tags mapped to this state
Expired	There should be no tags mapped to this state
Cancelled	There should be no tags mapped to this state
Terminated	There should be no tags mapped to this state

Set the current correction ID for all tags. Set the current correction ID to be the maximum correction ID listed on any part of the tag.

Set the TimeClassification for all Requests. The data is already present in E-Tag 1.7, so no translation is required.

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

System Requirements Document

Transmission System Information Networks (TSIN) Registry Rewrite

Version 1.0
August 22, 2006

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Revision History

Date	Version	Description	Author
December 13, 2005	0.3	Initial Version	JISWG
February 13, 2006	0.4	Addition of Glossary	JISWG
May 25, 2006	1.0	Changes to address Industry Comment	JISWG

Table of Contents

1 Introduction 1

1.1 Requirements Overview 1
1.1.1 Registry Identifier 2
1.1.2 Entities (Companies) 2
1.1.3 Clients (Users) 4
1.1.4 Security 4
1.1.5 Applications 4
1.1.6 Topology 6
1.1.7 Reference Documents 9
1.2 Glossary 9

2 Registry Processes and Procedures 12

2.1 General Concepts 12
2.2 Registry Administrator Procedures 12
2.2.1 Administrator Base Data 12
2.2.2 Full Registry Publication 13
2.2.3 V1.7 Registry Publication — Backward Compatibility 13
2.2.4 Tag Registry Publication 13
2.2.5 OASIS Registry Publication 14
2.3 Entity — Initial Registration 14
2.3.1 Entity 14
2.3.2 Entity Identifier 14
2.3.3 Entity Affiliate 15
2.3.4 Entity Predecessor 15
2.3.5 Entity Code and Entity Role 15
2.3.6 Entity Contact and Entity Code Contact 16
2.4 Entity — Updates 17
2.4.1 Entity 17
2.4.2 Entity Identifier 17
2.4.3 Entity Affiliate 17
2.4.4 Entity Predecessor 17
2.4.5 Entity Code and Entity Role 17
2.4.6 Entity Contact and Entity Code Contact 18
2.4.7 Entity Code Service 18
2.5 Entity – Deactivation 18
2.5.1 Entity 18
2.5.2 Deactivation of an Entity Code 18
2.5.3 Entity Role 19
2.6 Client — Initial Registration 19
2.7 Client — Updates 19
2.7.1 Client Role 19
2.8 Client — Deactivation 19
2.9 Application — Initial Registration 20
2.9.1 Application Services 20
2.9.2 Application Attribute Value 20
2.10 Application — Updates 21
2.10.1 Application Service 21
2.10.2 Entity Code Service 21

2.10.3 Application Service Contact 21
2.10.4 Application Attribute Values 21
2.11 Application — Deactivation 21
2.11.1 Application Service 21
2.11.2 Application Attribute Value 21
2.12 Topology — Initial Registration 22
2.12.1 Interconnection 22
2.12.2 Regional Reliability Organization 22
2.12.3 Reliability Area 22
2.12.4 Market Area 22
2.12.5 Balancing Area 22
2.12.6 Control Zone 23
2.12.7 Service Points 23
2.12.8 Paths 23
2.12.9 Adjacencies 24
2.13 Topology — Updates 24
2.13.1 Interconnection 24
2.13.2 Regional Reliability Organization 24
2.13.3 Reliability Area 24
2.13.4 Market Area 24
2.13.5 Balancing Area 24
2.13.6 Control Zone 25
2.13.7 Service Points 25
2.13.8 Paths 25
2.13.9 Adjacencies 25
2.14 Topology — Deactivation 25
2.14.1 Interconnection 25
2.14.2 Regional Reliability Organization 25
2.14.3 Reliability Area 25
2.14.4 Market Area 25
2.14.5 Balancing Area 26
2.14.6 Control Zone 26
2.14.7 Service Points 26
2.14.8 Paths 26
2.14.9 Adjacencies 26

3 User and Registry Interaction 27

3.1 Browser Interface 27
3.2 Encryption 27
3.3 Data Access Rights 27
3.4 Data Validation at Entry 27
3.5 Data Validation after Entry 27
3.6 Display Consistency 27
3.7 Color to Meaning Assignment 27
3.8 Application Programming Interface 27
3.9 Filtering and Sorting 28

4 Hardware and Software Standards 29

4.1 No Single Point of Failure 29
4.2 Data Backup and Storage 29
4.3 Disaster Recovery 29

4.4 Structured and Coordinated Upgrades 29
4.5 Sizing and Performance 29
4.5.1 Moderate Activity State 29
4.5.2 Heavy Activity State 30
4.6 Availability 30
4.7 Auditability 30
4.8 Data Integrity 30
4.9 NERC Cyber Security 30

5 Testing 31

5.1 Structured Test Document 31
5.2 Problem Reporting 31
5.2.1 Structured Problem Reporting 31
5.2.2 Problem Classifications 31
5.3 Factory Acceptance Testing 31
5.4 Factory Performance Testing 32
5.5 Site Acceptance Testing 32
5.6 Site Performance Testing 32

6 Documentation 33

6.1 Technical Documentation 33
6.2 User Documentation 33
6.3 Automated Interface Documentation 33

7 Training 34

7.1 Technical Training 34
7.2 User Training 34
7.3 API Training 34
7.4 Refresher and ongoing Training 34

8 Post Implementation Requirements 35

8.1 Problem Reporting and Enhancement Requests 35
8.2 System Upgrades 35
8.3 System Patches 35
8.4 Virus Detection Updates 36

1 Introduction

This System Requirements Document describes the content and requirements for a central repository (or Registry) of information that the electric industry needs in order to achieve both reliability and commercial interaction. The Registry must incorporate all existing functionality provided by the current TSIN Registry 1.7 and accommodate new industry requirements to support OASIS, NERC e-tag, and other applications. Data residing in the Registry must be authenticated before being published for use.

The Joint Interchange Scheduling Working Group, in cooperation with NERC staff, will oversee the development and implementation of the Registry.

1.1 Requirements Overview

The following is a brief summary of the existing regulatory and industry application requirements for information to be made available through a central registry:

- NAESB Business Practices Standards; Order 638
  - Entity Code
  - Entity DUNS
  - Transmission service attributes
  - Ancillary service attributes
  - Points of Receipt and Delivery (PORs/PODs)
- NAESB Standards and Communications Protocols for Open Access Same Time Information Systems (OASIS); Order 889-B, Order 605
  - OASIS Node Location (URL)
  - OTHER_CURTAILMENT_PRIORITY
  - PROCEDURE_NAME
  - PROCEDURE_LEVEL
  - REQUEST_TYPE
  - SECURITY_TYPE
  - SYSTEM_ATTRIBUTE
- NERC Reliability Standards and the NERC e-tag specification:
  - Tag Service Location (Agent/Authority/Approval/Forwarding URLs)
  - PSE Code
  - CA Code
  - TSP Code
  - SC Code
  - PORs/PODs
  - Sources/Sinks

The current TSIN Registry 1.7 definition accommodates most of these requirements.

The following are new Industry initiatives that could benefit from a central registry of information:

- NERC Functional Model
  - Functions performed by an entity (e.g., BA, TSP, etc.)
  - Certification of entity to perform function(s)
- NAESB Wholesale Electric Quadrant (WEC) Public Key Infrastructure (PKI)
  - Authorized Certification Authorities (CA)
  - Qualified CA Object Identifiers (OIDs)
  - CA Root Certificate Public Key

- e-tag Transaction Path Validation
  - TSP POR/POD Path and Scheduling Entity Association
  - TSP Path Adjacency
  - Source to TSP POR Adjacency
  - TSP POD to Sink Adjacency
- Seams Coordination and IDC Granularity
  - Book of Flowgates
  - AFC coordination data
  - Source/sink zones

These current and future Registry requirements are summarized in the following subsections according to the general functionality that will be required to be supported.

1.1.1 Registry Identifier

The Registry must include identifying information related to its publication, format, and applicability. Such information might include:

- Schema version
- Publication date/time
- Activation date/time

Schema version would reference an agreed to enumeration of revisions to the Registry, or might reference a specific XSD, if the Registry is published in an XSD form. Publication date would be when this version of the Registry was created and made available. Activation date would be when this specific version of the Registry was to take effect.

Additional information may be included to provide assurance that the Registry is authentic and has not been altered. This information might include a "digest" of the Registry, digitally signed by the registry administrator, such that any corruption or modification of Registry information could be detected. This mechanism will be determined during the detailed design phase of the Registry project.

1.1.2 Entities (Companies)

Entity (Company) registration is one of the key functions of the current Registry and will be extended in the new Registry. Key attributes that are required for entity registration and integration with existing applications include:

- Entity Name
- Entity Location(s)
- Entity Contact(s)
- Entity Identifier(s)
- Entity Code(s)
- Entity-to-Entity Relationship(s)
- Entity Role(s) (Functions)
- Entity Certification(s)

The Registry must support the registration of the full business entity name and primary place of business. Entity registration must provide for the entry of effective start and end date/times. These dates may be in the future to take effect on, but not before, the specified start date/time.

The ability to support a one-to-many relationship between a given registered entity and each of the attributes for location, contact information, identifiers, codes, affiliations and roles must be provided.

Entity location information will consist of a street address for the entity. Contact information will be classified by the contact type. Contact types will be defined in the Registry by the registry administrator.

For example, there may be administrative contacts, technical support contacts, emergency (24x7) contacts, etc. Contact types will be associated with the specific entity roles. The registry administrator may require that certain contact types be populated. The Registry implementation should enforce this requirement as part of automated data validation and constraint verification. Entity identifier would minimally support the registration of the entity's DUNS number required by the OASIS application. Various other industry recognized standard identifiers may be used in the future. The system design should anticipate the need to accommodate additional identifiers.

Entity code information is important to both the OASIS and the e-tag specifications. OASIS codes are the entity code itself. E-tag codes are the registered tag PSE codes currently consisting of the entity code with an appended tag desk code. (Note for additional description on entity codes)Current requirements must be supported, but other restrictions should be relaxed with the only requirement that entity code must be unique at any given point in time, and once assigned should have limited ability to be re-used by another entity, e.g., only in the case of an acquisition/merger or divestiture. The ability to require and enforce an authorized third party (i.e. Registry administrator or designee)[1] approval of registered entity codes must be included in the Registry.

Entity-to-entity relationships must be supported to provide a trace of entity acquisitions/mergers and or divestitures, as well as inter-entity affiliations. Entity affiliations are required by the OASIS application to identify the merchant affiliates of each transmission provider.

Entity roles or functions must be extended from the limited set supported by the current TSIN Registry 1.7 to support the registration of entities performing the various functions defined by the NERC Functional Model. Registration of an entity role/function should provide the ability for third party (i.e. Registry administrator or designee) approval or "certification" that the entity has in fact been qualified to perform that function. The ability to enable or disable the requirement for third party approval of a registered entity role is required. (Flag: "or information" will be added where appropriate.) The following are the initial set of entity roles to be considered in the Registry:

- Current O/SE (Operations) associated entity roles
  - RA — Reliability Authority/Coordinator (formerly Security Coordinator)
  - BA — Balancing Authority (formerly Control Area)
  - MO — Market Operator
  - TO — Transmission Operator
  - TSP — Transmission Service Provider
- Current TC/PSE (Merchant) associated entity roles
  - TC — Transmission Customer (i.e., OASIS customer code)
  - PSE — Purchasing Selling Entity (i.e., Tagging desk code)
  - LSE — Load Serving Entity (implies PSE)
  - GPE — Generation Providing Entity (implies PSE)
- Additional Entity Roles
  - Registry Administrator
  - ASP — Application Service Provider
  - PKICA — PKI Certification Authority
  - PKIPA — PKI Policy Authority
  - ERO — Electric Reliability Organization
  - RRO — Regional Reliability Organization
  - IMM — Independent Market Monitor
  - Other

[1] Note that "third party" identification depends on the type of information being registered.

The distinction of an entity being either an O/SE or TC/PSE should be retained for backward compatibility only. The key registration requirement is that an entity may register one or more entity codes. Each of those entity codes may be associated with one or more entity roles. The combination of entity code and entity role determines the context within certain actions that may be performed or granted. For example, in e-tagging, the entity code allowed to appear in association with a source must be designated as having the entity role of GPE to be valid in the context of that tag.

1.1.3 Clients (Users)

The Registry must support at least a rudimentary set of client/user registration functions to minimally identify who is able to access and update the Registry itself. There may also be requirements that certain applications will require the Registry to provide client authentication credentials, e.g., a Tag Agent client certificate registration.

The Registry must also provide a central repository to identify client credentials (e.g., certificate distinguished name, etc…) issued by all the authorized PKI certification authorities. This provides value for application system administrators in that they would not have to provide tools to access all the various PKI certificate repositories to gather this information. [2]The specific information to be retained in The Registry has not been finalized.

Typical information that would be registered for a client would include:

- User's entity
- User name
- User credential(s)

User credentials may include different types of credentials, but would minimally support the x.509 certificate information for one or more certificates issued to that client. The Registry must support a one-to-many relationship between a client and their credentials. Certificate credentials require information from the certificate subject field and certificate issuer field for uniqueness.

1.1.4 Security

The NAESB WEC PKI Certificate Policy and Authorized Certification Authority Accreditation and Certification program will identify those certification authority service providers that are authorized to issue certificates under the NAESB policy.

These certification authority service providers would be registered as an entity with the appropriate role of PKICA. An NAESB Policy Authority would be required to approve/certify these registrations before they are to be "trusted". Who will serve as the Policy Authority has not been determined. The following additional information will be registered for each authorized certification authority:

- Certificate Issuer(s)

The certificate issuers identify an attributes that can be embedded in the certificates issued by this authorized certification authority.

1.1.5 Applications

The Registry must support the registration of specific applications and will require the registration of specific "enumerated" data types or attributes. This requirement is particularly true for OASIS. FERC and NAESB Business Practice Standards enumerate specific transmission and ancillary service attributes and additional data elements that may be "registered" by a transmission provider.

[2] Note that The Registry must support the application validation identified in the electric industry PKI standard (NAESB PKI standards under development).

Applications may also require the identification or location of the server/service provided for the application. OASIS requires the registration of the OASIS node location (URL) for each transmission provider; e-tag requires the registration of the location (URL) for each of the tag services required to be provided by TSPs, CAs, and PSEs.

Each application that requires registration of specific information would appear in the Registry. Application "registration" is envisioned to be part of the base data established by the registry administrator. The specific application attributes would then be registered by either the industry at-large, or specific entities.

1.1.5.1 Application Services

The Registry currently supports registration of various application services by the Uniform Resource Locator (URL) that is used to access that service/application. This includes:

- OASIS Nodes
- Tag Agent Services
- Tag Authority Services
- Tag Approval Services
- Tag Forwarding Services

It is expected that additional services may be registered in the future. Such information might include locations for web services related service URLs, XML schema, WSDL, or UDDI locators.

Application services are envisioned to be registered and maintained by those entities that support/provide the service (e.g., entity type of ASP). Contact information should be provided for each service (e.g., twenty-four hour support, administrative, etc.). Many potential entities could subscribe or use these services. The Registry must support an entity's registration as a user/subscriber to a specific registered service. The Registry will need to support a many-to-many relationship between services and entities.

The Registry must support mapping between application services and the applications they support. The exact nature of this association must recognize the following types of existing relationships:

- Application = e-tag
  - Service = Tag Agent URL
  - Service = Tag Authority URL
  - Service = Tag Approval URL
  - Service = Tag Forwarder URL
- Application = OASIS
  - Service = OASIS URL
- Application = IDC
  - Service = IDC URL

1.1.5.2 Application Attributes

Each application appearing in the Registry may require the definition of unique registered attributes. OASIS requires such information for the transmission service attributes for data elements TS_CLASS, TS_TYPE, SERVICE_INCREMENT, etc. The e-tag application also requires definition of product codes and curtailment priorities.

Capabilities must be provided for a Registry administrator or designee to review and "approve" registration of attributes.

The basic information that is required to be captured related to application attributes would include:

- Application (name or identifier)

- Application Attribute (e.g., TS_CLASS, etc.)
- Application Attribute Value (e.g., FIRM, etc.)
- Registering Entity
- Approval Entity

1.1.6 Topology

The Registry must support the registration and association between physical, commercial, and reliability topology information for use in a variety of applications.

These applications would include:

- Definition of metered areas (balancing areas) controlled by registered balancing authorities (BAs)
- Definition of the metered areas (balancing areas) overseen by registered Reliability authorities/coordinators (RA) (reliability areas)
- Definition of metered areas participating in a centralized market overseen by a registered market operator (MO) (market areas)
- Contract path or e-tag path adjacencies between transmission providers (TSPs), and scheduling entities (SEs)
- Location of commercial service points (PORs, PODs, sources, or sinks) with respect to commercial markets and with respect to reliability related areas (BAs/RAs)
- Mapping of commercial service points to reliability or network modeled elements recognized by reliability applications (e.g., OASIS POR/PODs mapped to IDC flowgates or MMWG elements)

OASIS and e-tag currently require the registration of PORs, PODs, sources, and sinks and the association of Control Areas to Reliability Coordinators. This functionality must be retained and updated to reflect the NERC Functional Model. Registry administrator or designee (e.g., MO, TSP, or BA) approval of registered topology information must be supported.

The most significant immediate extension needed by the industry is a means to validate tag path information through the Registry. The requirements of this particular requirement are discussed in the following subsections along with some of the simpler topological relationships that may be represented in the Registry.

1.1.6.1 Interconnection

The Registry must provide for a hierarchical model of inter-relationships to represent the different topologies, physical, commercial, and/or political that is needed by the industry. Definition of the three major synchronous Interconnections, Western, Eastern, and ERCOT, must be included in the Registry as a foundational element. Creation and maintenance of Interconnection registration may be the responsibility of the registry administrator.

1.1.6.2 Regional Reliability Organization

Regional Reliability Organizations (RROs) may be included in the Registry to identify the overseeing RRO that has responsibility for a reliability area and/or balancing area.

RROs must be registered and associated with a single entity/entity code acting as that RRO. Registration of reliability areas and/or balancing areas as being associated with a given RRO must be supported. The possibility of a given reliability area being associated with more than one RRO must be supported.

1.1.6.3 Reliability Area

Reliability authorities/coordinators must have the ability to define their specific areas of influence. It is assumed that a reliability area would not cross an Interconnection. It may be related to one or more Regional Reliability Organizations and, it would include one or more balancing areas.

Reliability areas must be registered and associated with a single entity/entity code acting as reliability authority. The registry administrator may take on the responsibility for creating and maintaining registration of reliability areas.

1.1.6.4 Market Area

The boundaries of centrally administered markets may be registered. This information may be used by applications such as e-tagging to limit market operator re-dispatch of tagged transactions to only those balancing areas over which they have such authority. It is assumed that a market area can span one or more reliability areas, one or more Regional Reliability Organizations, but will contain, in its entirety, one or more balancing areas. The Registry must support market area registration. Market Operator adjustments would depend on this information.

Market areas must be registered and associated with a single entity/entity code acting as market operator. The registry administrator may take on the responsibility for creating and maintaining registration of market areas.

1.1.6.5 Balancing Area

The balancing area represents a named metered area overseen by a single certified balancing authority. It is assumed that a BA will be within one and only one Interconnection and one and only one market area (if any) and one and only one reliability area. The BA may span one or more Regional Reliability Organizations.

Balancing areas must be registered and associated with a single entity/entity code certified to act as a BA. The registry administrator may take on the responsibility for creating and maintaining registration of balancing areas.

1.1.6.6 Control Zone

The Registry must support the concept of control zones that represent subsets of a balancing area. This supports the potential for increased granularity for system reliability tools when identifying the impact of certain transactions on network elements. At least one control zone must be registered for each balancing area. Where increased model granularity must be recognized, the ability to associate multiple control zones within a single balancing area must be supported (e.g., PJM as balancing area has control zones of CE, AEP, DPL, etc.).

Control zones may be registered by the single entity/entity code certified to act as the BA that contains that control zone. Definition of control zones must be coordinated by those responsible for wide-area network modeling and maintenance of reliability tools that rely on those models. The registry administrator may take on the responsibility for creating and maintaining registration of control zones.

1.1.6.7 Service Points

The current Registry provides for transmission service provider definition of the commercial PORs and PODs used in OASIS. The Registry also provides for PSEs to define e-tag sources (for GPEs) and sinks (for LSEs). This functionality must be retained. However, a more rigorous process for Registry administrator or designee validation of these service point registrations should be instituted.

When registered, the relationship of each commercial service point to the entity making the registration (e.g., TSP for PORs/PODs), and the various “areas” in which the point is located (e.g., Interconnection, reliability area, market area, balancing areas, etc.) such that all the operational entities that may be involved with commercial or reliability issues associated with that point may be identified.

The Registry must provide for the association of a given source or sink with one and only one control zone. The Registry must also provide for the association of which registered entity/entity code of type

GPE may reference a given source and the association of which registered entity/entity code of type LSE may reference a given sink.

Currently, GPEs/LSEs are allowed to submit registrations of sources and/or sinks with approval granted to the referenced BA and/or MO. Since this information is so integrally tied into market and reliability processes and systems, the industry may elect to change the registration procedure to be controlled by operational entities rather than merchant entities. The Registry implementation must be flexible to allow control over source/sink registration by PSEs with approval of a balancing authority or market operator or limit registration to only be submitted and maintained by the BA/MO.

1.1.6.8 Paths

The Registry must support the definition of commercial transmission paths by each entity/entity code registered as a TSP. A path is defined as a valid POR and POD pair that may be scheduled with a designated scheduling entity (SE). There must be no restriction that a given named path may be associated with multiple POR/POD pairs, or that a given POR/POD pair may be associated with multiple paths. The combination of TSP, POR, POD, Scheduling Entity, and path name must be unique. Registration of paths and their associated POR/POD pair and Scheduling Entity must support the OASIS S&CP path naming convention.

For TSPs that have many Interconnections, physical and/or contractual, with other TSPs, the number of unique POR/POD pairs that represent valid commercial paths within their systems can be voluminous. The Registry implementation must provide for the ability to define paths using wildcard designations or other user interface or application programming interface structures to provide for an efficient mechanism to manage this large volume of information. The internal representation of path information in the Registry, however, may be very explicit to simplify programmatic use of the information.

That is, a TSP that has ten POR/PODs, and all possible pair-wise combinations of POR and POD are legitimate scheduling paths with a given Scheduling Entity, must be able to register and manage this information in an efficient manner even though the actual Registry may contain the explicit definition of the paths that result from those ten POR/PODs.

1.1.6.9 Path Adjacency

The Registry must support the ability to identify adjacencies between TSPs and Scheduling Entities'. This information is intended to be used specifically for e-tag scheduling path validations. Many constructs could be used to register and identify these adjacencies. The most direct method would be to identify which specific TSP registered paths (POR. POD, Scheduling Entity, Path combination) are adjacent to both any upstream TSP (i.e., TSP POR adjacent to upstream POD) and downstream TSP (i.e., TSP POD adjacent to downstream POR).

The Registry must recognize the many permutations of physical and contractual adjacencies that must be supported in order to accurately represent valid scheduling paths between TSPs and controlled by Scheduling Entities'. As with path definitions, this data can be voluminous and shorthand, efficient methods to enter and maintain the necessary associations must be implemented.

1.1.6.10 Source-POR Adjacency

The current source and POR registration must be extended to provide a mechanism to register the commercial relationship between a source resource and the TSP PORs over-which transmission service must be secured to schedule energy. Alternatively, source to path adjacency could be used to define this relationship more explicitly.

1.1.6.11 POD-Sink Adjacency

The current sink and POD registration must be extended to provide a mechanism to register the commercial relationship between a sink resource and the TSP PODs over-which transmission service

must be secured to schedule energy. Alternatively, source to path adjacency could be used to define this relationship more explicitly.

1.1.7 Reference Documents

The following reference documents provide additional information on the various functional requirements that must be met by the TSIN Registry 1.7.

- Standards and Communication Protocols for Open Access Same Time Information System (OASIS), Version 1.4, FERC Docket No. RM95-9-014.
- Open Access Same-Time Information System and Standards of Conduct, Order No. 638, FERC Docket No. RM95-9-0014.
- Master Registry Definition Document, Version 1.7, NERC.
- Electronic Tagging — Functional Specifications, Version 1.7.095, NERC.
- Electronic Tagging — Registry Definition, Version 1.7.04, NERC.
- NAESB WEC PKI Standard and Certificate Policy; pending approval of fNEASB.
- Registry Technical Specification, Version 2.0.3, NERC.

1.2 Glossary

Any definitions not contained herein may be found in the NERC Glossary of Terms Used in Reliability Standards (April 1, 2005), the NAESB WEQ Glossary, or FERC Glossary.

Application Programming Interface (API) – A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol.

Application Service Provider (ASP) – An **ASP** is a business that provides computer-based services to customers over a network. The most limited sense of this business is that of providing access to a particular application program (such as medical billing) using a standard protocol such as HTTP.

Balancing Authority (BA) – The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

Certification Authority (CA) – The organization that issues and manages certificates.

Certificate issuer – The Certification Authority

Certificate OID – Each certificate policy is uniquely represented by an "object identifier" (OID) which is a numeric string that is contained in a field of each certificate that is issued according to a given certificate policy. In order to ensure interoperability and uniqueness of each OID, these are registered with recognized international bodies according to a structure defined in X.208 from the International Telecommunications Union (ITU) (the structure can be examined at http://www.alvestrand.no/objectid/top.html).

Client certificate – X.509 Digital Certificate received (by a “client”) from a Certification Authority.

Digital certificate – The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called "digital IDs," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as VeriSign (www.verisign.com) and Thawte (www.thawte.com). The CA verifies that a public key belongs to a specific company or individual (the "subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.

Data Universal Numbering System®(DUNS) – The **Data Universal Numbering System®**, abbreviated as **D-U-N-S®** , is a system developed and regulated by Dun & Bradstreet (D&B) which

assigns a unique numeric identifier to a single business entity. This numeric identifier is commonly referred to as a D-U-N-S number.

Electric Reliability Organization – Responsible organization authorized under the Federal Power Act to develop and enforce Reliability Standards that provide for an adequate level of reliability of the Bulk-Power System.

Entity affiliate – An organization that is associated with another organization as a subordinate, subsidiary, or member.

Entity predecessor – The organization that preceded the current organization. This typically follows a reorganization, merger, acquisition, or divestiture.

Extensible Markup Language (XML) – A metalanguage written in SGML that allows one to design a markup language, used to allow for the easy interchange of documents on the World Wide Web.

Generation Providing Entity (GPE) – Merchant selling energy from owned, affiliated, or contractually bound generation.

Global attribute – Industry defined attributes such as TS_CLASS FIRM.

Independent market monitor – An organization that is not affiliated with any electric industry Market Participant, Market Operator, or Transmission Service Provider that is responsible for monitoring market activities.

Load-Serving Entity (LSE) – Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Local attribute – An attribute defined by the TSP such as SERVICE_INCREMENT SEASONAL.

Market Operator(MO) – Entities registered as market operators and serving as either source or sink for a TRANSACTION may exercise such functions in order to indicate correct flow based on market clearing.

PKI certification authority (PKICA) – In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many public key infrastructure (PKI) schemes.

Point Of Delivery (POD) – A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.

Point Of A Receipt (POR) – A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.

Policy Authority – The entity that has ultimate responsibility for approving the Certificate Policy used to govern the issuance, management and usage of a specified set of digital certificates

Reliability Authority/Coordinator (RA/RC) – The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator’s vision.

Root CA identifier – Unique OID of the Root CA.

Root CA Public key – The pubic key of the Root Certificate Authority X.509 digital certificate that is provided to the Root CA’s subordinate Certificate Authorities.

Root Certificate – In cryptography and computer security, a **Root Certificate** is an unsigned public key certificate, or a self-signed certificate, and is part of a public key infrastructure scheme. The most common commercial variety is based on the ISO X.509 standard. Normally an X.509 certificate includes a digital signature from a certification authority (CA) which vouches for correctness of the data contained in a certificate.

Scheduling Entity (SE) – An entity responsible for approving and implementing Interchange Schedules.

Transmission Operator (TO) – The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.

Transmission Service Provider (TSP) – The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.

Unaffiliated entity – Any of two or more organizations that are not associated with each other as a subordinate, subsidiary, or member.

Uniform Resource Locator (URL) – The address that defines the route to a file on an Internet server (Web server, FTP server, mail server, etc.). URLs are typed into a Web browser to access Web pages and files, and URLs are embedded within the pages themselves as hypertext links.

2 Registry Processes and Procedures

2.1 General Concepts

Due to the industry's heavy reliance on the existing TSIN Registry 1.7 in the e-tag application, implementation of a new Registry should consider it essential to maintain full backward compatibility to re-create the existing Registry schema and publication mechanisms (Access MDB and CSV files).

Every Registry entry must also support tracking of the following key information:

- Creation Date – date/time the entry was first inserted into the Registry
- Activation Date – date/time the entry becomes active or in use
- Deactivation Date – date/time the entry is no longer to be used
- Last Update – date/time the registry was last updated
- Modified By – identifying information for the person or software application that created/modified the Registry entry

The registry design must also consider providing a general mechanism to audit Registry changes and reconstruct the Registry at a given point in time. Consideration should be given to a uniform database table update process whereby the record to be updated is marked as 'deactivated' and the updated data inserted as a new record with a corresponding 'activation' date/time.

2.2 Registry Administrator Procedures

2.2.1 Administrator Base Data

Certain base data information will need to be established and maintained by the registry administrator. Such information might include:

- Entity Identifier Types — DUNS, etc.
- Entity Role Types — BA, LSE, ASP, etc.
- Client Role Types — Entity Admin, Registry Admin, etc.
- Contact Types — Administrative, 24-Hour, Technical Support, etc.
- Applications — OASIS, e-tag, etc.
- Application Service (Server) Types — OASIS, Tag Agent, etc.
- Application Attributes — TS_CLASS, SECURITY_TYPE, etc.
- Interconnections — Eastern, Western, ERCOT
- Regions — MAAC, WECC, etc.
- Service Point Role Types — Source, POD, etc.

Additions, updates, and deletions (deactivation) of records within these tables will be restricted to the registry administrator only. The user interface will allow the registry administrator to view, add, and modify records in these tables as necessary. General access to these tables by all other users will be restricted to read only access. Addition of new information in these tables may be initiated by industry participants through an off-line administrative procedure with appropriate "checks and balances" as established by the registry administrator.

Until a PKI policy authority is identified, the registry administrator, under the direction of the NAESB Certificate Policy, will assume sole responsibility for maintaining the content of the following Cyber-Security related base data:

- Certificate Root – Authorized Certification Authority (CA) Root Certificate
- Certificate Policy – Authorized CA OID(s) for certificates issued
- Certificate Issuer – Distinguished name of Authorized CA Issuing Authority(ies)

2.2.2 Full Registry Publication

The registry administrator is responsible for the periodic publication of the full Registry and potentially selected subsets of that registry. The publication of the registry requires taking a snapshot of the Registry at the time indicated in the Registry Version and Publication Date field. The Registry will then be made available for download in the following formats:

- XML via defined web services using SOAP encapsulation and XML schema(s)

The current publication frequency is:

- Registry published daily at midnight.
- Published Registry's activation date set for midnight twenty-four hours after publication.

The new Registry may need to be published more frequently than the current TSIN Registry. This publication schedule may change in the future dependent on how frequently Registry data is modified.

The Registry may be cleaned of all spurious data corrections made between publications due to mistakes, typos, etc., made during the registration process. The registry administrator may archive all records whose creation date AND deactivation date is greater than the last publication date but less than the publication date (i.e., records that never became active in the Registry).

Rather than periodic publication of the Registry on a fixed schedule, the registry administrator may elect to only publish a new Registry when information has changed since it was last published. The ability for any registered entity/entity code to subscribe for notification of the availability of a new Registry must be provided.

2.2.3 V1.7 Registry Publication — Backward Compatibility

The implementation of the new Registry requires 100% backward compatibility with the existing NERC V1.7 Registry publication methods to minimize the immediate impact on existing production applications that rely on the Registry. The Registry Detailed Design Specification must describe the mechanism for reconstituting the contents of the various V1.7 Registry table records from the new Registry's schema.

Coincident with the publication of the full Registry, automated procedures will be executed to convert that Registry information into the V1.7 Registry Microsoft Access database ".mdb" file and to generate all associated Comma Separated Values CSV files. The V1.7 Registry database and "CSV" files will be published on the same frequency as the full Registry. The registry administrator will also execute and/or review the results of a record-by-record comparison of the new V1.7 Registry with that published previously to determine if there are any obvious errors in the conversion process.

Note that in retaining backward compatibility, features added specifically for the new Registry (e.g., PKI certificate information) will not be accessible through the V1.7 * ".mdb" or * ".csv" files. Applications will need to be updated to read the new V2.0 Registry information published in XML format available via web services, since the backwards compatibility will only be maintained for 18 months from the go live date of the new Registry.

2.2.4 Tag Registry Publication

The NERC e-tagging specification requires only a subset of pertinent information from the full Registry. Coincident with the publication of the full Registry, a subset of Registry information may be made available for use by tagging application service providers. This data will be provided in CSV file format consistent with the currently provided e-Tag CSV Registry data for backwards compatibility for 18 months. During this time the users of this data will need to convert over to the new V2.0 Registry information published in XML format available via web services.

2.2.5 OASIS Registry Publication

The OASIS application requires only a subset of pertinent information from the full Registry. Coincident with the publication of the full Registry, a subset of Registry information may be made available for use by OASIS application service providers. This data will be provided in CSV file format consistent with the currently provided OASIS version 1.4 CSV Registry data for backwards compatibility for 18 months. During this time the users of this data will need to convert over to the new V2.0 Registry information published in XML format available via web services.

2.3 Entity — Initial Registration

The following information must be collected as part of the initial registration process for a new entity:

- User — information regarding the individual submitting the initial entity registration; this information will populate an initial client associated with the entity and assigned the role of "Entity Administrator" (See Client – Initial Registration);
- Entity — information including official/legal entity name, business address, etc.;
- Entity Code — one or more short acronyms to be associated with the entity with one or more entity role(s) can be assigned to each entity code;
- Entity Identifier — one or more industry recognized legal entity identifiers (e.g., DUNS) if any entity code assigned the role of TSP (transmission service provider), or TC (transmission customer). Additional validations/requirements may depend on other roles assigned to the entity ;(Determined at a later date.)
- Entity Affiliates — zero or more identifications of any active, registered entities to which the new entity is affiliated;
- Entity Predecessor — zero or more associations to existing registered entities, which gave rise to formation of the new entity (e.g., merger, acquisition, divestiture, etc.).

The following subsections describe specific requirements relative to the validation and processing of the entity's initial registration.

2.3.1 Entity

The entity's official/legal name must be verified for uniqueness. Desired "activation date" will default to the Registry Version Activation Date unless an alternative date in the future is supplied by the user (activation date in the past must be flagged as an error).

The activation date will apply to all entity related information records inserted into the Registry during initial registration.

Prior to insertion into the database, a unique master registry identifier must be assigned to the entity being registered. This identifier should be used as the reference identifier in all data registered by that entity. Changes in information such as entity address, etc., should not constitute registration of a new entity. Mechanisms must be supported that allow the transfer of all existing registered information associated with one entity to another through a user request.

2.3.2 Entity Identifier

Entity identifier information submitted must supply both the value for the identifier (e.g., DUNS number) along with the "type" of identifier represented by that value (e.g., "DUNS"). Entity identifier information submitted must be verified for uniqueness. If the entity has attempted to register an entity code with entity role of TSP or TC, the registration information must contain a DUNS number as at least one of their entity identifiers to comply with OASIS registration requirements.

2.3.3 Entity Affiliate

Entity affiliate information, if any, must verify that the affiliated entity is still a valid/active entity. Entities and affiliates must mutually approve the establishment of the relationship.

2.3.4 Entity Predecessor

Entity predecessor information, if any, must verify the validity of the preceding entity registration(s). This information would most likely be presented and submitted from the UI when the user seeks to change an existing registered entity to reflect merger, divestiture, etc. If an existing entity is being replaced, both the predecessor and the successor must agree to this relationship. Predecessor entities do not necessarily have to be active to be associated with a new entity registration.

Along with identifying any predecessor entity, the reason for the change in entity registration must be identified from a set of enumerated reasons including:

- Merger
- Acquisition
- Divestiture
- Reorganization
- Other

2.3.5 Entity Code and Entity Role

At least one entity code must be provided and associated with at least one entity role. The entity role of "unaffiliated entity" (or any of its specific associated roles) must be the only entity role selected and be associated with only a single entity code, i.e., unaffiliated entities are limited to one registered entity code and only the role of "unaffiliated entity".

For backward compatibility, only one entity code may be identified as "O/SE" (operations or security entity) and only one entity code may be identified as "TC/PSE". This entity code represents the V1.7 Registry records in the Entity Registration table, and corresponds to the transmission service provider and transmission customer codes used in the OASIS application (e.g., SELLER and CUSTOMER data elements).

There is no restriction on a given entity registering separate entity codes as both an "O/SE" and "TC/PSE". If not explicitly supplied, the O/SE and/or TC/PSE role will be assumed by default for the first entity code registered that has one or more of the specific O/SE or TC/PSE roles defined as shown below. In addition, the role of PSE will be assumed if either GPE or LSE is selected.

- Current O/SE (Operations) associated entity roles
  - RA — Reliability Authority (formerly Security Coordinator)
  - BA — Balancing Authority (formerly Control Area)
  - MO — Market Operator
  - TOP — Transmission Operator
  - TSP — Transmission Service Provider
  - IA – Interchange Authority
  - GO – Generator Operator
- Current TC/PSE (Merchant) associated entity roles
  - TC — Transmission Customer (i.e., OASIS customer code)
  - PSE — Purchasing Selling Entity (i.e., Tagging desk code)
  - LSE — Load Serving Entity (implies PSE)
  - GPE — Generation Providing Entity (implies PSE)

- Other Functional Model Roles
  - GOP – Generator Operator
  - GO – Generator Owner
  - TO – Transmission Owner
  - PA – Planning Authority
  - TP – Transmission Planner
  - RP – Resource Planner
  - DP – Distribution Provider
- Additional entity roles
  - Registry Administrator
  - ASP — Application Service Provider
  - PKICA — PKI Certification Authority
  - PKIPA — PKI Policy Authority
  - ERO — Electric Reliability Organization
  - RRO — Regional Reliability Organization
  - IMM — Independent Market Monitor
  - Other

Certain restrictions may be required that would make some combinations of entity roles mutually exclusive, i.e., registration of an entity code as both a TSP and PSE may be invalid. All submitted entity codes must be verified for uniqueness. Prior to insertion into the Registry, a unique master registry identifier may be assigned to each of the Entity Codes being registered.

The capability to designate an entity with registration approval rights over the registered entity code/entity role must be provided unless the entity code is registered with any of the entity role of "other". These entities may represent regulatory agencies, universities, consulting groups, etc., that do not have an active merchant or operations role in the electric industry. These entity registrations may be required to designate a Sponsoring Entity (i.e., one with merchant or operations role) that will serve as the registrant's approval entity. Alternatively, the registry administrator may take on this approval role.

Following submission of the registration of an entity code table, as a triggered event or controlled by a batch script procedure, e-mail notifications must be generated to the administrative contact for the entity identified as having approval rights over the entity code registration. Similarly, once an entity code registration has been approved, an e-mail notification must be sent to that entity's administrative contact.

2.3.6 Entity Contact and Entity Code Contact

Registration of contact information must be provided at both the entity level and at the entity code/role level. User information identifying the registrant will be used to create an initial client record associated with the new entity registration. By default, entity contact and entity code contact information create a mapping of this client to the "Administrative" contact for the entity as a whole and for each supplied entity code. The administrative contact will then be responsible for adding additional client records in association with the various contacts, which may be associated with the entity and/or entity code(s) after the initial registration (e.g., 24 hour, Technical Support, etc.).

The following enumerated contact types must be supported:

- Administrative
- Technical
- 24 hour
- Operations — Real-time
- Operations — Day-ahead/pre-schedule
- Customer relations

Not all contact types are required or applicable to each of the various entity roles. Certain contact types may be required by industry standards and practices in association with specific entity roles, and such requirements must be modeled in the Registry.

2.4 Entity — Updates

2.4.1 Entity

Authorized "Entity Administrators" may update information associated with their entity registration. These updates would be to legal business entity name and/or location. Update operation is effected by deactivating the current record and inserting a new record with the updated information activated coincident with the deactivation of the original record. Entity relationships within the various registered objects must key to unique identifiers assigned to the entity and maintained across updates to that entity's registered information and not to specific table record identifiers. This ensures that the Registry contains both current and all historic records associated with the entity. Similar constructs must be applied to all registered objects.

2.4.2 Entity Identifier

New entity identifiers may be registered by authorized entity administrators. Entity identifiers may be updated to reflect corrections or changes in the value of any registered identifier by first deactivating the current registered information and then inserting the updated information into the entity identifier table.

2.4.3 Entity Affiliate

New entity affiliate associations may be inserted by authorized entity administrators. New information will be verified in the same manner as performed for the initial entity registration. Termination of entity affiliate relationship records is accomplished by updating the deactivation date field to reflect when the affiliation was terminated, and may occur at any time without restriction. There is no information that may be updated with respect to entity affiliation.

2.4.4 Entity Predecessor

New entity predecessor associations may be inserted by authorized entity administrators. New information will be verified in the same manner as performed for the initial entity registration. Entity predecessor information is restricted to being registered by the succeeding entity only. Modification of existing information will be accomplished by deactivating the current information and inserting the updated/corrected information.

Deletion of entity predecessor records is accomplished by updating the deactivation date field to reflect when the association between the entities was terminated; this is assumed to mainly be the result of correcting an error on registration.

2.4.5 Entity Code and Entity Role

Updates to entity code information are restricted to the addition or deactivation of entity role information. The entity code itself may only be altered if it has not been approved, and is subject to all uniqueness checks as described for initial entity registration.

New entity code and entity role associations may be submitted for an existing entity. Entity code and entity role information will be validated to insure it passes all validations as described for a new entity registration.

Entity code and entity role associations must support the ability to track approval of that code/role by an authorized third party, i.e., NERC would have approval of entities registering with the balancing authority role as part of their certification program.

See discussion below for restriction on deactivation of entity code or entity role information.

2.4.6 Entity Contact and Entity Code Contact

Contact information associating entity or entity code/role with a client may be added, updated or deactivated. Updating an entity contact or entity code/role contact record to reference a new client must result in deactivation of the existing record and insertion of a new record. Deactivation of an entity contact or entity code contact record may occur at any time without restriction. Insertion of new entity contact or entity code contact records requires only that the associate client record is currently active.

2.4.7 Entity Code Service

Certain entity codes must be mapped to appropriate application services (servers), e.g., PSEs mapped to TagAgent Server, TSP mapped to OASIS Server, etc. The entity administrator may insert, update or deactivate entity code service registrations at anytime without restriction. Update of entity code service associations is accomplished by deactivating the current record and inserting a new entity code service association. Note that the actual service registrations are performed by the entity providing that service.

2.5 Entity – Deactivation

The following subsections describe specific constraints or requirements for deactivation of Entity and related Registry information.

2.5.1 Entity

Deactivation of an entity requires the simultaneous deactivation of all associated records containing the following information/associations:

- Entity affiliate associations
- Entity codes
- Entity contacts
- Entity identifiers
- Clients

Each of these may have further constraints or requirements for deactivation of associated records.

Presence of active records associated with the entity to be deactivated for the following information will block deactivation of the entity. The user/administrator must deactivate these records prior to attempting to deactivate the entity.

- Services (for ASP entities)
- Certificate root (for PKICA entities)
- Certificate issuer (for PKICA entities)

2.5.2 Deactivation of an Entity Code

Entity code requires the simultaneous deactivation of all the following associated registry information:

- Entity roles
- Entity code contacts
- Entity code services
- Entity code service points (for TSP, GPE and LSE entities)
- Entity code paths (for TSP entities)
- All topology related mappings to entity code

Each of these may have further constraints or requirements for deactivation of associated records.

2.5.3 Entity Role

Deactivation of an entity role associated with a given entity code is subject to the following constraints:

- If the entity role to be deactivated is an entity role type of RA or SC, there must be no active reliability area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of BA or CA, there must be no active balancing area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of MO, there must be no active market area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of TSP, there must be no active POR/POD, path or path adjacency registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of PSE, there should be no active source/ sink associated with the entity code
- If the entity role to be deactivated is entity role type of ASP, there must be no active application service registrations associated with the entity code

Any such active registrations referencing an entity role to be deactivated must first be deactivated or assigned to another entity code prior to deactivation of the entity role record.

2.6 Client — Initial Registration

Submission of client information is subject to uniqueness and validation checks. Initial registration of an entity always must result in insertion of an active client record associated with the role of entity administrator. At a minimum, client registration information will be used for Registry Access Control.

Submission of client information may be performed by clients associated with active, approved, registered entities where the client has been assigned the role of user administrator. All information is subject to uniqueness and validation checks. Information required for registration of a client includes designation of name and contact information. Additional information may be submitted to define associated:

- Client certificates (or more generic client credentials)
- Client roles

Contact information associated with entities, entity codes, or services may be modeled as registered clients and mapped to entity, entity code, or service and contact type information, or maintained separately from the client registration.

Prior to insertion into the database, a unique master registry identifier must be assigned to the client being registered.

2.7 Client — Updates

2.7.1 Client Role

Association/disassociation of roles to an active client may occur at anytime without restriction. Now, the only roles envisioned are those required to implement Registry Access Control, including but not limited to:

- Entity administrator
- User administrator

2.8 Client — Deactivation

Deactivation of a client record is subject to the following constraints and/or requirements:

- All active client role records associated with the client to be deactivated must be deactivated simultaneously

If client registrations are used to identify contacts, the following additional constraints are required:

- All active entity contact registrations associated with the client to be deactivated must be deactivated simultaneously
- All active entity code contact records associated with the client to be deactivated must be deactivated simultaneously
- All active service contact records associated with the client to be deactivated must be deactivated simultaneously

2.9 Application — Initial Registration

The only application related registration information accepted from external entities is registered Application Services and Application Attribute Values. All other application related registry information is maintained by the registry administrator. This includes the identification of the registered applications and associated application service types (e.g., e-tag Tag Agent Service).

2.9.1 Application Services

Submission of service registration information may be performed by clients of an active, approved registered entity with at least one entity code assigned the role of ASP. All information is subject to uniqueness and validation checks.

Information required for registration of a service includes designation of the service type, URI, and a description. Additional information may be submitted to identify one or more service contact information (e.g., technical support, etc.).

Prior to insertion into the database, a unique master registry identifier must be assigned to the service being registered.

2.9.2 Application Attribute Value

Submission of application attribute value information includes the name of the application as defined in the application base data and the particular data element whose value is being registered as defined in the application attribute name base data.

Currently, submissions of application attribute values are only allowed for the OASIS application and may only be submitted by clients whose parent entity contains an active, approved entity code designated with the entity role of TSP.

The application attribute base data defines whether the application attribute value is subject to approval by another entity and which entity is granted approval rights. If approval is not required, the registry administrator will be the approval entity and the registered value will be automatically approved on insertion into the database.

If approval is required, an e-mail notification must be sent to the administrative contact(s) associated with the approval entity. Once that entity updates the record to indicate approval (or disapproval), an e-mail notification will be sent to the registering entity's administrative contact.

Attributes that require approval must be considered ‘global’ attributes that any TSP may reference or use (e.g. TS_CLASS). Attributes not requiring approval must be considered ‘local’ and apply only to the entity that registered that attribute value.

2.10 Application — Updates

2.10.1 Application Service

Authorized ASP entity administrators may update information associated with their service registrations. These updates would be to service URL or description. Update operation is effected by deactivating the current registration and inserting a new record with the updated information.

2.10.2 Entity Code Service

Addition, update or deactivation of registered entity code service associations are controlled by the entity owning that entity code. Activation of new records or deactivation of existing records may occur at any time without restriction. Update of existing records, i.e., changing service association, must be accomplished by deactivating the current record and inserting a new record with the updated information.

2.10.3 Application Service Contact

Contact information associated with a service may be added, updated or deactivated. Updating a service contact registration will result in deactivation of the existing record and insertion of a new record. Deactivation of a registered service contact may occur at any time without restriction.

2.10.4 Application Attribute Values

Once registered, OASIS application attribute value registrations may only be deactivated by the entity that approved the registration. The registering entity may update the value and associated description fields prior to approval of the registration only, i.e., for correction of errors or on the advice of the approval entity. Once approved, no updates will be allowed except for deactivation by the approval entity. Transmission and ancillary service attributes are examples of OASIS attributes, which require oversight and approval. Once these attributes are registered by one TSP, they must be re-useable by any other TSP. This would prevent unnecessary duplication of effort and eliminate a possible source of inconsistencies.

Certain OASIS application attributes are private to the TSP (local), such as REDUCTION_TYPE, SYSTEM_ATTRIBUTE, etc. No Registry administrator or designee approval is required for these attributes, and they may be updated by the entity that registered the attribute.

2.11 Application — Deactivation

2.11.1 Application Service

Deactivation of a registered application service is subject to the following constraints and requirements:

- All application service contact records associated with the service to be deactivated must be deactivated simultaneously
- Any active entity code service associations to the service to be deactivated must block deactivation of the service

The Registry may support the registration of application services, which are ‘voluntary’ in nature. These services may be registered, updated and deactivated at will by the registering entity without affecting operations of any other services.

2.11.2 Application Attribute Value

Registered application attribute value records may be deactivated as described in the update process at any time. Global attributes must be deactivated by the entity that approved the registration; local attribute values may be deactivated by the registering entity.

2.12 Topology — Initial Registration

The following subsections outline the basic processes required for initial registration of topology information.

2.12.1 Interconnection

The registry administrator will assume responsibility for establishing the base definitions for the electrical system synchronous interconnections.

2.12.2 Regional Reliability Organization

The registry administrator will assume responsibility for establishing the base definitions for the Regional Reliability Organizations at the direction of NERC.

2.12.3 Reliability Area

A registered and approved (by NERC) reliability authority must have the ability to register a reliability area. Key attributes are:

- Area name
- Association to the Reliability Authority
- Association to one or more Balancing Areas

The entity that approved the registration of the reliability authority must also have the rights to define the reliability area on the RAs behalf.

The registry administrator at the direction of NERC will most likely establish the initial set of Reliability authorities/coordinators and areas.

2.12.4 Market Area

A registered and approved market operator must have the ability to register a market area. Key attributes are:

- Area name
- Association to the market operator
- Association to one or more balancing areas

The entity that approved the registration of the market operator must also have the rights to define the market area on the MOs behalf.

A validation rule must be enforced that a given balancing area may not appear in multiple market areas.

2.12.5 Balancing Area

A registered and approved (by NERC) balancing authority must have the ability to register a balancing area. Key attributes are:

- Area name
- Association to the balancing authority
- Association to one or more control zones
- Association to the market area (if any)
- Association to one reliability areas
- Association to one or more Regional Reliability Organization (optional)

The entity that approved the registration of the balancing authority must also have the rights to define the balancing area on the BAs behalf.

The registry administrator at the direction of NERC will most likely establish the initial set of balancing authorities and areas.

2.12.6 Control Zone

Control zones are subsets of balancing areas that allow reliability tools, such as IDC, have increased granularity over transaction impacts than for the balancing area as a whole. Control zone definitions require coordination between NERC, network modeling groups, reliability tool developers, etc.

A registered and approved (by NERC) balancing authority must have the ability to register a control zone. By default, each balancing area must have one control zone registered whose name is identical to the parent balancing area. Key attributes are:

- Zone name
- Association to the balancing area
- Association to one or more service points (sources/sinks)

The entity that approved the registration of the balancing authority must also have the rights to define the control zone on the BAs behalf.

The registry administrator, at the direction of NERC, will most likely establish the initial set of balancing areas and control zones.

2.12.7 Service Points

NAESB Business Practice Standards require registration of PORs and PODs by TSPs. Key attributes include:

- Point name
- Role (POR and/or POD)
- Association to the transmission service provider

No approval should be required for an entity code with role of TSP to register PORs and PODs.

Registration of sources and sinks is currently handled by purchasing selling entities with approval granted by the balancing authority. Provisions must be made to allow sources and sinks to be registered directly by the balancing authority or market operator (for BAs within their market) in coordination with the PSE(s). Key attributes include:

- Point name
- Role (source and/or sink)
- Association to one or more purchasing selling entity
- Association to the control zone

PSEs associated with a source point must have the additional entity role of GPE; PSEs associated with a sink point must have the additional entity role of LSE.

No approval should be required for an entity code with role of TSP to register PORs and PODs.

2.12.8 Paths

To support tag path validation, TSPs will be required to register all valid commercial transmission service paths and their associated upstream and downstream adjacencies. Key elements of a registered path are:

- Path name
- POR
- POD
- Association to the transmission service provider

- Association to the scheduling entity

Paths are uniquely identified by the combination of all five attributes. Due to the large volume of data this represents for each TSP, the UI forms for registering paths must make efficient use of wildcards.

The OASIS S&CP identifies the following sub-attributes of a standardized path name:

- Region code
- Provider code
- Path code
- Optional code
- Spare code

2.12.9 Adjacencies

Path and source/sink adjacency information must be registered by the TSP. Path adjacency information would indicate:

- Association to upstream path
- Association to downstream path

Source adjacency information would indicate:

- Association to source service point
- Association to downstream path

Sink adjacency information would indicate:

- Association to upstream path
- Association to sink service point

2.13 Topology — Updates

2.13.1 Interconnection

The registry administrator will assume responsibility for performing any updates on the definitions for the electrical system synchronous Interconnections.

2.13.2 Regional Reliability Organization

The registry administrator will assume responsibility for performing any updates on the definitions for the Regional Reliability Organizations at the direction of NERC.

2.13.3 Reliability Area

The reliability authorities or the entity that approved the RAs registration must be able to update the registration of the reliability area. This would be limited to changing the area name, the associations of balancing areas to the reliability area, and assignment of responsibility from the current owning reliability authority to another approved RA.

2.13.4 Market Area

The market operator must be able to update the registration of the market area. This would be limited to changing the area name, the associations of balancing areas to the market area, and assignment of responsibility from the current owning market operator to another approved MO.

2.13.5 Balancing Area

The balancing authorities or the entity that approved the BAs registration must be able to update the registration of the balancing area. This would be limited to changing the area name, the associations of

control zone(s) to the balancing area, and assignment of responsibility from the current owning balancing authority to another approved BA.

2.13.6 Control Zone

The balancing authorities or the entity that approved the BAs registration must be able to update the registration of the control zone. This would be limited to updating the control zone's name, or adding/removing source sink points.

2.13.7 Service Points

TSPs must have the ability to update their POR/POD service point registrations.

BAs and or MOs whose balancing areas are under the control of the MO must have the ability to approve and/or update their source/sink service point registrations.

2.13.8 Paths

TSPs must have the ability to update their path registrations.

2.13.9 Adjacencies

TSPs must have the ability to update the path adjacencies associated with any of the TSPs defined paths. Adjacency registration should be coordinated by the adjacent entities and responsibility delegated to one or the other parties to avoid conflicts.

TSPs must also have the ability to update the path to source/sink adjacencies in coordination with the source/sink balancing authority.

2.14 Topology — Deactivation

2.14.1 Interconnection

The registry administrator will assume responsibility for performing any deactivations of the definitions for the electrical system synchronous Interconnections.

2.14.2 Regional Reliability Organization

The registry administrator will assume responsibility for performing any deactivations of the definitions for the Regional Reliability Organizations at the direction of NERC.

Deactivation of a Regional Reliability Organization will simultaneously deactivate all associations of the RRO to balancing authorities (if any).

2.14.3 Reliability Area

The reliability authority or the entity approving the RA must have the ability to deactivate a reliability area.

Deactivation of a reliability area will simultaneously deactivate all associations of the RA to balancing authorities (if any).

2.14.4 Market Area

The market operator must have the ability to deactivate a market area.

Deactivation of a market area will simultaneously deactivate all associations of the MO to balancing authorities (if any).

2.14.5 Balancing Area

The balancing authorities or the entity that approved the BAs registration must be able to deactivate the registration of the balancing area. Deactivation of the balancing area must simultaneously deactivate the area's associations to registered RROs, reliability areas, and/or market areas. Deactivation must be blocked if there are any active control zones associated with the balancing area.

2.14.6 Control Zone

The balancing authorities or the entity that approved the BAs registration must be able to deactivate the registration of the control zone. Deactivation of the control zone must simultaneously deactivate the zone's associations to register the balancing area. Deactivation must be blocked if there are any active service points associated with the control zone.

2.14.7 Service Points

TSPs must be allowed to deactivate service points. Deactivation of a POR/POD must be blocked if the service point is associated with an active path. . Deactivation of a source/sink must simultaneously deactivate that point's association with the control zone, and any of the point's path adjacencies.

2.14.8 Paths

TSPs must be allowed to deactivate paths. Deactivation of a path must simultaneously deactivate any path adjacencies referencing that path.

2.14.9 Adjacencies

TSPs must be allowed to deactivate path adjacencies at will.

3 User and Registry Interaction

3.1 Browser Interface

The registry shall implement a web browser user interface, allowing users to access and manually register and enter data into the Registry without requiring any special software installations.

3.2 Encryption

The vendor shall allow (or require) the user to use 128 bit SSL.

3.3 Data Access Rights

Users (including programmatic users via API) shall be allowed access to data based on their registered and approved data access rights. Registered users will be allowed only read access rights to data "belonging" to other entities (as described in section 2). Users may only modify, delete, or create data what "belongs" to them. NERC may initiate deletion of invalid data according to the procedures described in section 2.

3.4 Data Validation at Entry

The system shall validate data content and format on data entry wherever possible providing meaningful error messages to the user that will allow the user to determine how to correct the data entry error.

3.5 Data Validation after Entry

The accuracy and validity of registry entries MUST be verified by automated and/or manual processes prior to use by industry participants. Prior to populating the "production" or "active" Registry, updates to the Registry must be confirmed with the appropriate stakeholders. The vendor will work with NERC to determine the appropriate data validation procedures and practices and then optimize the efficiency of this validation.

3.6 Display Consistency

Display formats and function must be consistent across all displays. NERC staff will have final authority on determining if the vendor has met these requirements. If NERC believes that the display is deficient in some manner, then they will provide the vendor with a specific description of what the vendor must change in order to achieve compliance with this requirement.

3.7 Color to Meaning Assignment

If the registry imparts information by color, then this color should be used to mean the same thing on all displays. For example, if the color RED is used to show a data format problem, it must not also be used to highlight data in an "accepted" state.

3.8 Application Programming Interface

The registry will provide the ability to upload data to and download data from the Registry using XML files defined by a published XML schema. Standards consistent with e-tag and WECC's EIDE system shall be used including, SOAP, SMXP, and GMT for time representation. Any XML schemas used in the API must be provided to NERC for public distribution. The XML API shall use 128 bit SSL.

The registry shall also provide registry data in a CSV file format that can be downloaded using https. The SSL required for this download is 128 bit.

For backward compatibility, all methods available today to download the registry data files (Access and CSV formats) shall continue to be supported until this backward compatibility requirement is removed eighteen months from the publication of version 2.0.

3.9 Filtering and Sorting

All user data displays must include filter and sort capability as appropriate.

Columns in displays shall all be able to be sorted in both ascending and descending order by any column (i.e. Source, Sink, POR, POD, etc.).

Displays shall all be able to be filtered based on the values in any meaningful column. Numeric columns shall be filterable based on both absolute and range values. Text columns must be filterable based on partial string matches and exact matches with negation. String filtering shall not be case sensitive. It shall be possible to enter up to 20 text strings for a single field that shall be logically "OR"d together.

Examples:

- PointID=6007,
- NERCID between 511 and 801,
- POR contains NYPD,
- PSE does not contain ENRN,
- POD = MALN OR CAPJ.

4 Hardware and Software Standards

4.1 No Single Point of Failure

The Registry shall be designed so that there are no single points of failure that would result in the Registry being unavailable for greater than one hour. For example, the system could be fully redundant with hot standby/failover functions. This availability requirement extends to the Internet connections, which could also be redundant and through two, independent Internet service providers. All failover, including network failover, must be automatic.

The Registry shall be designed so that there is no single point of failure that would result in the loss of Registry data for greater than one hour. For example, disks could be mirrored and configured in an array with hot spares.

Internet and Registry system redundancy could be satisfied by replication between diverse sites.

4.2 Data Backup and Storage

The Registry data must be backed up at least daily, with data being moved offsite at least weekly. The data must be under the protection of access controls such that no single employee has access to the offsite data storage. Management approval must be required to access the offsite data. There are no historical data storage requirements other than what is needed for disaster recovery.

4.3 Disaster Recovery

The Registry system must be capable of being restored entirely assuming the destruction of the entire registry system. Documentation and procedures must be available that provide for the complete re-installation/re-construction of the Registry hardware, software, and data. The registry must demonstrate that the documentation and procedures are accurate by having NERC staff perform or witness the building of the system from scratch.

4.4 Structured and Coordinated Upgrades

Upgrades/modifications to any component of the Registry that would affect the users must be coordinated with NERC staff and the Registry user community. Upgrades that would change an API must be implemented following a structured implementation plan. This plan must include reasonable periods of at least three weeks for the Registry users to have access to the revised XML schema or whatever else is necessary for the Registry users to implement and test changes in their automated systems. The three-week period must be followed by two weeks of testing with a near-continuous test Registry available for the users to test against. This system must be populated with either test, or actual data.

4.5 Sizing and Performance

The system must be sized and designed so that it provides robust performance for both current and expected usage.

- CPU utilization, averaged over one minute, must be below 20% 95% of the time.
- Disk space utilization at full expected size of the Registry must be 50% or less.
- RAM must be sized sufficiently on all systems (including database servers) so that disk swapping does not exceed 20 pages per minute.

4.5.1 Moderate Activity State

Display call up times and API retrieval times shall be measured when the system is in a *moderate activity state*, carrying out normal functions, while 50 users simultaneously use the interface for normal activities and the API is being used by 50 systems to retrieve data.

Under this loading state:

- User displays call up and display change must not exceed five seconds (excluding internet latency and browser start up times).
- Response to SOAP method calls shall be within five seconds.

4.5.2 Heavy Activity State

Display call up times and API retrieval times shall be measured when the system is in a *heavy activity state*, carrying out *peak* normal functions, while 50 users simultaneously use the interface for normal activities and the API is being used by 150 systems to retrieve data.

Under this loading state:

- User displays call up and display change must not exceed ten seconds (excluding internet latency and browser start up times).
- Response to SOAP method calls shall be within ten seconds.

4.6 Availability

The Registry must be available 99.5% of the time measured over any rolling 30-day period.

4.7 Auditability

The database and registry systems must be auditable. While maintaining records with start/stop dates partially accomplishes this goal, other values need to be tracked for audit purposes. These at a minimum include the user requesting data modifications (inserts, updates, deletes), timestamp, and similar information for the approval/authorization process (NERC staff member/timestamp) for example. XML input documents must also be retained for a configurable number of days.

4.8 Data Integrity

Database and data integrity must be guaranteed. The registry can choose from a number of different tools and procedures to ensure this.

4.9 NERC Cyber Security

The Registry and related components are critical to both operational and commercial sectors of the power industry. As such, NERC classifies the entire system as a Critical Cyber Asset and requires that the registry and any subsequent entities maintaining the Registry comply with applicable NERC CIP standards.

5 Testing

5.1 Structured Test Document

The vendor shall provide a structured test document that tests all functional and performance requirements of the Registry. NERC staff and, at NERC's option, NERC members, may review the document and provide input and corrections which must be incorporated prior to the start of structured testing. The test document must contain numbered sections consistent with the system requirements document so that testers may easily reference required functionality and compare it to rest results.

5.2 Problem Reporting

The vendor shall provide a structured method of reporting, classifying, and tracking problems.

5.2.1 Structured Problem Reporting

Each identified possible problem shall be assigned a unique number and assigned a classification.

5.2.2 Problem Classifications

Problems will be classified as:

- R — Required Functionality (In the System Requirements Document)
- E — Enhancement (Identified as necessary but not in the System Requirements Document)
- B — Bug (Software or Hardware Problem)
- D — Disputed (Agreement cannot be reached)

Problems will further be classified as:

- C — Critical (Required for system to be considered operational)
- H — High priority (Not required but very important)
- M — Medium priority
- L — Low priority

5.3 Factory Acceptance Testing

Factory Acceptance Testing (FAT) shall be conducted on-site. Certain client functions may be tested remotely at the client facilities.

The FAT will consist of both structured testing and unstructured testing. Structured testing will be conducted first.

Unstructured testing will include testing of any required functions in any order at any loading level.

FAT may be conducted several times. Passing FAT is defined as completion of structured and unstructured testing without finding any problems above those classified as low priority.

FAT testing will continue until the NERC staffs or vendor staffs determine that system problems are so severe that no further testing should be done until the problems are corrected.

At completion of FAT testing, if FAT is not passed, the vendor shall correct all problems classified above low priority and another FAT shall be started. This will include re-testing of functions already tested since corrections of problems may cause problems elsewhere in the system.

The vendor will perform a minimal set of FAT and provide results of that testing to NERC before scheduling on site FAT. (Hopefully minimizes travel to on-site location)

5.4 Factory Performance Testing

Factory Performance Testing (FPT) shall be conducted on-site. Certain client functions may be tested remotely at the client facilities.

The FPT will consist of confirmation that the system meets sizing and performance requirements. The vendor will be responsible for loading the system to both the medium and heavy activity state. NERC staff will have ultimate approval and confirmation rights that these activity states are met for the duration of the appropriate performance tests.

Either the vendor or the NERC staff may devise mutually agreeable timing tests (including the use of a stopwatch, performance monitors, or software timers).

5.5 Site Acceptance Testing

Site Acceptance Testing (SAT) shall be conducted at the Registry host facility (ies). Client functions will be tested remotely at the participating client facilities.

SAT is a repeat of FAT with the exception that passing SAT is defined as completion of structured and unstructured testing without finding *any* problems. SAT testing will be open to any NERC member.

5.6 Site Performance Testing

Site Performance Testing (SPT) shall be conducted at the Registry host facility (ies). Certain client functions may be tested remotely at the client facilities.

SPT is a repeat of FPT.

SPT *may be* waived by NERC at their discretion.

6 Documentation

The vendor will be responsible for providing hardware and software documentation. NERC staff shall have approval rights over all documentation provided. The documentation requirements are not waived if the successful vendor provides the Registry service via an application service provider. For example, technical documentation, meeting the requirements described herein, will still be required to be provided to the vendor's own technical staff in this case.

NERC must have the capability to modify and maintain the documentation described in this section or the vendor must maintain it. The intent is that the documentation be kept up to date as changes are made to the Registry system.

Frequently Asked Question (FAQ) documents must also be created and made available online. Provisions must be provided so that these may be maintained on an ongoing basis.

6.1 Technical Documentation

The vendor shall provide NERC with technical documentation describing the hardware architecture and software architecture of the system. The intent of the technical documentation is to allow NERC or their appointees to maintain the system. Since a number of methods are possible for describing the system, including UML, DFD's, etc, there will be no specific requirement in this document as to the form of this documentation. The only requirement is that the intent be met.

6.2 User Documentation

The vendor shall provide the Registry users with user documentation that describes how the client interface is used and all of its possible functions. NERC staff will have approval rights over this documentation.

The documentation must be provided online at the Registry site. Documentation on user registration must be provided online at the NERC Web site.

Documentation must include examples where appropriate.

6.3 Automated Interface Documentation

The vendor shall provide NERC with API documentation that describes, in detail, how users may install and/or utilize the API to the Registry. Any related XML schemas shall be provided to the users so that they may implement their own XML processor independent of any specific vendor solution.

The documentation must be provided online at the Registry site.

Documentation must include examples where appropriate.

7 Training

The vendor will be responsible for providing training courses. NERC staff has approval rights over course content and quality. The vendor must provide courses that meet NERC approval. Training must be presented both in person and online via webex.

These classes may need to be presented in a variety of locations over a number of different days in order to provide access to all Registry users. NERC staff will coordinate training class locations and dates with NERC members and ensure that all NERC members are provided with access to training.

7.1 Technical Training

The vendor shall provide technical training to NERC staff or their appointees in order to assure that they have sufficient knowledge to maintain the system (depending on the final roles) and interact with it (for data confirmation, deletion procedures, etc.).

7.2 User Training

The vendor shall provide training to the Registry users so that at the end of the course, the users are proficient at using the client interface and understand all of its functions.

7.3 API Training

The vendor shall provide technical training to Registry users on the use of the API so that the users, at the end of the course, have a thorough understanding of the interface and how to use it.

7.4 Refresher and ongoing Training

The vendor will provide updated training for system upgrades and changes so that ongoing training may be conducted and available.

8 Post Implementation Requirements

The vendor will be responsible for providing a number of services after implementation of the Registry. All upgrades or modifications to software described in this section must be implemented following requirements outlined in previous sections 4.0, 5.0, 6.0 and 7.0 of this document.

8.1 Problem Reporting and Enhancement Requests

The vendor shall provide a mechanism for both NERC staff and NERC members to report and classify problems and enhancement requests. These will be assigned priority levels by NERC members and staff as follows:

- C — Critical (Required for system to be considered operational)
- H — High priority (Not required but very important)
- M — Medium priority
- L — Low priority

They will also be assigned a classification as follows:

- E — Enhancement
- B — Bug (software or hardware problem)
- D — Disputed (Agreement cannot be reached)

The vendor will allocate resources to correct the identified problems consistent with the priority level assigned as follows:

- C = Immediate mitigation effort required and will be continuous until problem is resolved. Daily status updates from the vendor will be required.
- H = Mitigation efforts must start no later than the next working day and continue during normal working hours until complete. Daily status updates from the vendor will be required.
- M = Mitigation efforts must start within the next ten working days. Vendor will provide an estimate for completion acceptable to NERC Staff. Staff and vendor will work together to prioritize “M” issues. Weekly status updates from the vendor will be required.
- L = Vendor will provide an estimate for completion acceptable to NERC staff. Staff and vendor will work together to prioritize “L” issues. Weekly status updates from the vendor will be required.

8.2 System Upgrades

NERC staff or the vendor, with agreement from NERC staff, may initiate system hardware and/or software upgrades in order to remain current with external vendor support levels (such as the operating system, programming language, or database vendor) or improve performance or reliability.

Responsibilities for staff performing the upgrades need to be established with the vendor in the Registry contract or according to sections 4.0, 5.0, 6.0 and 7.0 of this document as a minimum.

8.3 System Patches

NERC staff and the vendor must establish a method by which critical operating system patches, database system patches, and any other applicable patches required for ensuring system security, implementing bug fixes, and implementing enhancements will be applied. Patches that correct security issues must be applied as soon as possible. Patch application must conform to NERC Cyber Security standards.

8.4 Virus Detection Updates

Virus detection software must be installed and continuously running on the Registry computer systems. NERC staff and the vendor must establish a method by which virus detection software is updated. Updates must be downloaded and applied daily.

Item 3. TSIN Registry Transition from NERC to NAESB

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Request for Information

Transmission System Information Networks (TSIN) Registry Rewrite

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Table of Contents

1. Introduction **1**

2. Response Procedure **2**

3. Background **3**

3.1 North American Electric Reliability Council (NERC) 3
3.2 Project Scope 3
3.2.1 Summary of the TSIN registry 4
3.2.2 Summary of the new Registry 5
3.2.3 Additional Considerations 5
3.3 Expected Features 5
3.4 NERC-specific Requirements 6
3.4.1 Security 6
3.4.2 Data 6
3.4.3 Hardware and Development Languages 6

4. Questions for Vendor Consideration **7**

4.1 Interactions with NERC 7
4.2 Access Control 7
4.3 Access Request Module 7
4.4 Data Input 7
4.5 Data Output 7
4.6 Auditability 8
4.7 Technical Requirements 8
4.8 Vendor Requirements 8
4.9 Price 8
4.10 Quality 9
4.11 Development, Testing, and Training 9
4.12 Other 9

1 Introduction

The North American Electric Reliability Council (NERC) seeks to develop a new software application to replace its existing Transmission System Information System (TSIN) registry. NERC is issuing this Request for Information (RFI) to gauge vendor interest in providing software development services, to estimate budget impacts to accomplish said development, and to project a development timeline. Within this RFI, the new software application will be referenced as the Registry.

This RFI and the referenced System Requirements Document (SRD)describe the known requirements for the Registry. These requirements are the result of a needs analysis conducted by the electric industry's Joint Interchange Scheduling Working Group (JISWG), the North American Electric Standards Board (NAESB), and the North American Electric Reliability Council (NERC).

This document contains the following sections: 1) an explanation of the response procedure; 2) project scope and background information; 3) a description of NERC's business requirements 4) technical requirements; 5) vendor requirements; 6) questions regarding potential price and the pricing structure; and, 7) questions regarding the quality of the package.

2 Response Procedure

Responses to this RFI are due by close of business on **September 29, 2006**. All responses must be in electronic format, Microsoft Word (Office 2000 or later) or Adobe Acrobat (Version 6.0 or later) and delivered via email or postal mail to NERC's Project Manager, whose address is provided below.

NERC plans to use responses to this RFI to estimate the budgetary requirements and development schedule for this project. Therefore, vendors are asked to be as thorough as possible in their responses. Reponses may include supporting documentation, e.g. white papers.

Prospective vendors are asked to provide the following information with their responses to this RFI:

Responding Company Information	
Company Name:	
Contact name:	
Address:	
City:	
State/Province	
ZIP/Postal code:	
Country:	
Phone number:	
Fax number:	
Email:	

Please send responses to the following address. Please note that the preferred method of communication is by email.

Subject: Registry Rewrite

Brian Nolan
Manager Information Technology and Projects
Off: 1-609-452-8060
Fax: 1-609-452-9550
Email: Brian.Nolan@nerc.net

North American Electric Reliability Council
Princeton Forrestal Village
116-390 Village Boulevard
Princeton, New Jersey 08540-5731

3 Background

3.1 North American Electric Reliability Council (NERC)

NERC is a nonprofit corporation whose members include eight regional reliability councils. The members of these councils come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied and used in the United States, Canada, and a portion of Baja California Norte, Mexico.

A ten-member, independent Board of Trustees, including the CEO, governs NERC with guidance and input from an industry Stakeholders Committee. The Stakeholders Committee elects the independent trustees, votes on amendments to bylaws, participates in the budget process, and provides advice and recommendations to the board on policy matters. The Board of Trustees provides governance oversight and strategic direction to the NERC management team and staff.

In fulfilling its mission, NERC performs the following critical functions:

- Sets standards for the reliable operation and planning of the bulk electric systems.
- Monitors, assesses, and enforces compliance with standards for bulk electric system reliability.
- Conducts regular "readiness" audits of all reliability coordinators, control areas, and other bulk electric system operators to ensure they are capable of complying with NERC standards.
- Supports excellence in electric system operations through accreditation of operator training programs and certification of system operators and operating organizations.
- Provides education and training resources to promote bulk electric system reliability.
- Assesses, analyzes, and reports bulk electric system adequacy and performance.
- Coordinates reliability standards and procedural matters with regional reliability councils and other organizations.
- Coordinates the provision of applications (tools), data, and services necessary to support the reliable operation and planning of the bulk electric system.
- Takes a leadership role in critical infrastructure protection of the electricity sector.
- Responds promptly and investigates major bulk electric system emergencies.
- Enables the reliable operation of the interconnected bulk electric systems by facilitating information exchange and coordination among reliability service organizations.
- Administers procedures for appeals and conflict resolution for reliability standards development, certification, compliance, and other matters related to bulk electric system reliability.

In addition, NERC monitors and participates in the regulatory proceedings of federal, state, and provincial government agencies on issues pertaining to reliability. NERC also provides advice and guidance to government agencies upon request, serves as a technical resource for federal and state government officials, and participates in related conferences and programs.

The NERC office is located in Princeton, New Jersey. NERC's staff of approximately 60 professionals works with the technical committees and their subgroups to provide project coordination and support. (Each regional council has its own staff.)

3.2 Project Scope

The attached System Requirements Document (SRD) for the new Registry contains details on the expected content and requirements for the Registry, which is intended to replace in entirety NERC's

existing TSIN registry. The Registry must incorporate all functionality provided by the current TSIN registry and accommodate new industry requirements to support OASIS, electronic tagging, and other applications. Furthermore, the new Registry must communicate with other pre-defined NERC data structures and fit into NERC's computing environment. Prospective vendors must be willing to work with NERC personnel for this purpose.

3.2.1 Summary of the TSIN registry

The current TSIN registry supports two industry applications: OASIS and Electronic Tagging. The web-based registration tool and data repository have been in use since 1996. Original requirements were contained in FERC Open Access Same-time Information System (OASIS) rulemaking (see FERC Docket No. RM95-9-003 – Open Access Same-Time Information System Standards and Communications Protocol.) Additional functionality has been added to the TSIN registry to support the original and subsequent versions of the Electronic Tagging specification (see http://reg.tsin.com/Tagging/e-tag/).

Entities required to register information with TSIN include: Transmission Customer/Purchasing-Selling Entities (TC/PSE), Operating/Security Entities (O/SE), OASIS Node Information Providers, and Observer. These groups of entities are defined as follows:

Transmission Customer/Purchasing-Selling Entities (TC/PSE)

> Any eligible company or business entity (or its designated agent) that can or does execute a transmission service agreement or can or does receive transmission service.

Operating/Security Entities (O/SE) (transmission providers, balancing authorities, and reliability coordinators)

> Transmission Provider (TP) – A public utility company or entity (or its designated agent) that owns, operates, or controls facilities used for the transmission of electric energy in interstate commerce.
>
> Balancing Authority (BA) – An electric system or systems, bounded by interconnection metering and telemetry, capable of controlling generation to maintain its interchange schedule with other balancing authority and contributing to frequency regulation of the Interconnection.
>
> Reliability Coordinator (RC) – An entity that provides the reliability assessment and emergency operations coordination for a group of balancing authorities. Reliability Coordinators do not participate in the wholesale or retail merchant functions.

OASIS Node Information Provider

> A Transmission Provider or agent to whom the Transmission Provider has delegated the responsibility of meeting any of the requirements of providing the information system to support OASIS requirements for a set of Transmission Providers.

Observer

> An entity able to view information on OASIS nodes.

TSIN contains information about the following:

- Reliability Coordinators
- Balancing Authorities
- Transmission Providers
- Purchase Selling Entities
- MRD Flowgates
- POR and POD Point names

- Transmission Products
- Source and Sink Point names
- Etag provider URLs

Once per day, NERC posts a set of data files created from TSIN data for download by industry participants. Many participants have automated the process of downloading these files and integrating the data into back-end systems.

3.2.2 Summary of the new Registry

Changing industry needs coupled with advances in technology are driving the need for the new Registry. While incorporating new requirements and functionality to meet those needs, the new Registry must continue to meet the needs of existing applications (e.g. OASIS and Electronic Tagging.) It must be scalable and extensible to accommodate future enhancements. The Registry must integrate seamlessly within NERC's computing environment. It also must communicate with existing data stores to reduce duplication and improve overall user experience.

The System Requirements Document (SRD) for the new Registry (Attachment A) defines the desired content and functionality of the new Registry and describes the testing, documentation, and training requirements. A vendor would be required to create a companion Technical Specification document describing the software design, database architecture, and necessary data flows to a sufficient level of detail to allow project developers, management, and selected reviewers to agree on the fundamental design.

The SRD contains the following sections related to the major components of the Registry:

- Registry Processes and Procedures – describes the functionality necessary to add new information and revise existing information in the Registry.
- User and Registry Interaction – describes the requirements of the user interface displays and data entry forms required to provide the functionality defined in the Registration Processes and Procedures.
- Hardware and Software Standards
- Testing
- Documentation

The functions described in the SRD must be implemented in an easily maintainable and flexible framework that may expand to accommodate additional functionality with minimal impact to existing functions. Backward compatibility with TSIN output formats and publication schedules must be ensured.

3.2.3 Additional Considerations

NERC desires a turn-key rather than an application as a service approach. Prospective vendors must be willing to work with NERC to integrate the new Registry into NERC's existing computing infrastructure.

3.3 Expected Features

The following features must be incorporated into the Registry, at a minimum:

- Customizable and definable user access levels.
- User name and password access controls.
- Administrative section for manage access controls.
- A module or modules for user information registration. The purpose of this module or these modules is to provide the Registry users a method of entering entity, client, application, and topological information for a given entity.
- A module for publishing the Registry.

- A module that addresses data validation.
- A module that addresses the application programming interface (API) interactions with the Registry.

3.4 NERC-specific Requirements

3.4.1 Security

Due to the nature of the data that is contained within the Registry and the relationship to other data stores in NERC and the system availability requirements, NERC requires that the Registry implementation comply with NERC Cyber Security Standard CIP 002 through CIP-009, or its successor standards, from a software perspective.

3.4.2 Data

All data contained within the Registry will remain the property of NERC. At no time should a vendor expect access to Registry data for any purpose other than those defined by NERC. During considerations of this RFI, prospective vendors must account for safeguards that NERC will require to prevent unauthorized release of information.

3.4.3 Hardware and Development Languages

NERC will retain ownership of all data and software developed for this project. Contracts will be structured so that venders are contracted to develop a tool, implement the tool in the NERC IT environment, and then provide maintenance and support for a pre-determined period of time.. During the RFI process, vendors are asked to propose hardware necessary to meet the availability requirements and any system software licenses. NERC will have the option of:

- Having the vendor procure all the hardware and software licenses, or
- Independently procuring all or using existing components or licenses.

Acceptable platforms are as follows:

- Operating Systems: Windows Server 2003®, or later
- Database: SQL Server 2000 or later

Acceptable Development Languages are as follows:

- Microsoft VB.NET
- HTML
- MS SQL

If a platform or development language not listed above is required to provide the optimal solution, please specify in your response.

4 Questions for Vendor Consideration

NERC requests prospective vendors to review and respond to the following series of questions. The purpose is twofold. First, answers will help NERC identify issues that it must address before a Request for Proposal can be prepared. Second, prospective vendors' consideration of these questions can help determine their level of interest in developing a proposal for NERC should a request be forthcoming.

4.1 Interactions with NERC

1.	How would you approach the integration of the new Registry into NERC's existing computing environment and manage data flows between existing NERC data stores?
2.	What would you require of NERC for this purpose and at what stages of this project?

4.2 Access Control

1.	How would you anticipate implementing Access Control in the Registry?

4.3 Access Request Module

Per FERC, access to this tool must be open. Privacy is dictated once an entity has been vetted for inclusion i.e. has a valid DUNS number.

1.	How will users request access to the tool?
2.	How will representatives of NERC approve their access?

4.4 Data Input

1.	How would you handle the loading of existing TSIN data into the new Registry?
2.	Would you consider providing the ability to "bulk" load data as a feature of the system? If so, how do you envision that process?
3.	What form of automated data validation will the Registry use?
4.	How will new data, changes to data, and removal of data be handled?

4.5 Data Output

1.	How would you meet the Registry publication requirements described in the SRD?
2.	How do you anticipate meeting the backward compatibility requirements?

4.6 Auditability

1.	How do you anticipate meeting the auditability requirements of the Registry?

4.7 Technical Requirements

1.	Will you be able to develop this application in the designated development language? If not, please tell us the development language and reason for use.
2.	Do you think the required functionality can be delivered in stages? If so, what would be the priority order of implementation?
3.	How will a link with Microsoft Office be implemented?
4.	Do you believe the requirements for scalability and expandability can be met? Please explain.
5.	How do you envision the change management process?
6.	How would a search function be integrated?
7.	How would you envision incorporating on-line help, and how would you address the need to keep help content current? ?

4.8 Vendor Requirements

1.	How do you support software implementations?
2.	Would NERC's data confidentiality requirements pose problems?
3.	What reassurances can you make regarding data confidentiality?

4.9 Price

1.	Given the requirements noted in this RFI and in the SRD, what would you consider a reasonable system development cost? Would pricing options be available?
2.	Could the number of users affect the price?
3.	Would you include source code? If not, how would its inclusion affect the price?
4.	Is the creation of databases and standard interfaces included in your price? How?
5.	According to your experience, what is your estimated total cost for implementing?

6.	Please provide a summary of your estimated costs, to include upfront development costs, ongoing maintenance costs, and monthly service and support costs.

4.10 Quality

1.	How many days of training can be expected? Break out into areas.
2.	Please provide a list of suggested performance metrics (i.e. defects, labor cost for maintenance…)

4.11 Development, Testing, and Training

1.	What is the estimated time to develop this tool? Break out into phases, if possible.
2.	What is the estimated time required for testing this tool?
3.	How will training on this tool be handled for NERC personnel?
4.	Would you consider user training an option and if so, how would you accomplish it?

4.12 Other

1.	Do you consider any of the requested functionality technically unfeasible, or too complex to implement? If so, please explain.
2.	Do you believe the SRD contains enough detail to translate into a technical specification for application development? If not, please identify areas that you think require additional detail.
3.	Would you expect any part of the software to be labeled vendor-proprietary? If so, please explain.
4.	Would publishing the Registry schema and API's be problematic for you? If so, please explain.