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

Interchange Subcommittee Meeting
and
Joint Interchange Subcommittee Working Group Meeting

Marriott Portland City Center
520 Southwest Broadway
Portland, OR 97205
Phone: (503) 226-6300

Wednesday, May 2, 2007 — 8 a.m.–5 p.m.
Thursday, May 3, 2007 — 8 a.m.–noon

Conference Bridge Participation (Phone Call In)
Phone Number: (732) 694-2061
Access Code: 1123050207#

Agenda

1. Administrative

a. Membership and Guests — Chair
b. Arrangements — Secretary
c. Approval of Meeting Minutes:
   i) February 14-15, 2007, IS – JISWG Meeting Minutes — Chair
   ii) March 16, 2007, E-Tag 1.8 Vendors Meeting Minutes — Chair
d. Procedures
   i) Parliamentary Procedures — Chair
   ii) Antitrust Compliance Guidelines — Chair
e. Interchange Subcommittee Action Items List (Review prior to the meeting) — Chair

2. Working Group Reports

Working Group Meetings, Conference Calls, or Action Since the Last IS Meeting

a. Joint Interchange Scheduling Working Group (JISWG) — Jim Hansen, Bob Harshbarger

3. NERC Reliability Standards

a. Urgent Action SAR (INT-005-2, INT-006-2, INT-008-2) — Don Lacen
b. FERC Standards Order, Extract for INT Standards — Tom Vandervort

4. E-Tag 1.8

a. E-Tag 1.8 Implementation Plan Posting – Respond to Comments – Don Lacen

5. WECC Interchange Milestones

a. Western Interconnection Tool (WIT) Update — Don Lacen
b. WECC Standards Waivers — Don Lacen

6. IS – ORS Joint Meeting

a. Dynamic Schedule Information in the IDC — Don Lacen, Jim Castle
b. Reliability Standard INT-006-1 — Don Lacen, Jim Castle
c. Conditional Firm Service — Don Lacen, Jim Castle

7. Future Meetings

a.	September 19-20, 2007	Montreal
b.	November 14-15, 2007	San Francisco
c.	February 20-21, 2008	Date and Location - To Be Determined
d.	May 21-21, 2008	Date and Location - To Be Determined
e.	September 17-18, 2008	Date and Location - To Be Determined
f.	November 19-20, 2008	Date and Location - To Be Determined

Item 1.a Membership and Guests

Vice-Chair Don Lacen will welcome the Interchange Subcommittee (IS) and Joint Interchange Scheduling Working Group (JISWG) members and guests. The acting chair will ask members and guests to introduce themselves.

Each member is asked to check and review the current Interchange Subcommittee roster for accuracy.

Attachments

1. Interchange Subcommittee Roster

Item 1.b Arrangements

The Resources Subcommittee meeting will begin on Wednesday, May 2, 2007 at 8 a.m. and adjourn by noon on Thursday, May 3, 2007. Lunch will be served on Wednesday.

Item 1.c Approval of February 14-15, 2007 and March 16, 2007 Meeting Minutes

The chair will ask for approval of the IS - JISWG February 14-15, 2007 meeting minutes and the IS – JISWG E-Tag 1.8 Vendor March 16, 2007 meeting minutes.

Attachment

1. February 14-15, 2007 IS – JISWG Meeting Minutes
2. March 16, 2007 IS – JISWG, E-Tag 1.8 Vendor Meeting Minutes

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 Interchange Subcommittee Action Items List

Discussion

The action items list is attached for the subcommittee to review prior to the meeting. The action item list will not be reviewed during the meeting. However, the chair or any member can discuss specific items or request assistance to close them.

Action

Between meetings, the subcommittee is to review the action item list on a periodic basis and perform necessary tasks to close the items. The subcommittee secretary will schedule meetings, conference calls, and webcasts to support efforts to address the action items. It is the responsibility of the action figures to address and close their items.

Attachment

Interchange Subcommittee Action Items List

Item 2. Working Group Reports

Some or all of the subcommittee working groups may have met or conducted conference calls since the last meeting to discuss their respective issues and concerns.

Items 2.a–2.d Working Group Reports

Discussion and Action

The IS work groups' chairmen will report to the subcommittee regarding deliverables, significant investigations, action items, and concerns that are new or carry-over from the last meeting.

Work Group	Task Force Chairs
Joint Interchange Scheduling Work Group	Jim Hansen and Bob Harshbarger

Item 3. NERC Reliability Standards

Item 3.a Urgent Action SAR (INT-005-2, INT-006-2, INT-008-2) – Don Lacen

The initial ballot for the Urgent Action SAR to modify the timing table in the following Coordinate Interchange Standards was conducted from Monday, March 19, 2007 through Friday, March 30, 2007.

INT-005-2 – Interchange Authority Distributes Arranged Interchange

INT-006-2 – Response to Interchange Authority

INT-008-2 – Interchange Authority Distributes Status

The Urgent Action SAR will correct an error in the timing table that appears in all three standards. Under some conditions, the error in the timing table doesn't give reliability entities within WECC enough time to conduct a reliability-related review of e-tags.

For additional information, check the NERC Standards web site.

Ballot Results

Quorum:	85.54%
Weighted Segment Vote:	96.82%
Ballot Results:	The Standard has passed

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

(Docket No. RM06-16-000; Order No. 693)

Mandatory Reliability Standards for the Bulk-Power System

(Issued March 16, 2007)

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Final Rule.

SUMMARY: Pursuant to section 215 of the Federal Power Act (FPA), the Commission approves 83 of 107 proposed Reliability Standards, six of the eight proposed regional differences, and the Glossary of Terms Used in Reliability Standards developed by the North American Electric Reliability Corporation (NERC), which the Commission has certified as the Electric Reliability Organization (ERO) responsible for developing and enforcing mandatory Reliability Standards. Those Reliability Standards meet the requirements of section 215 of the FPA and Part 39 of the Commission's regulations. However, although we believe it is in the public interest to make these Reliability Standards mandatory and enforceable, we also find that much work remains to be done. Specifically, we believe that many of these Reliability Standards require significant improvement to address, among other things, the recommendations of the Blackout Report. Therefore, pursuant to section 215(d)(5), we require the ERO to submit significant improvements to 56 of the 83 Reliability Standards that are being approved as mandatory and enforceable. The remaining 24 Reliability Standards will remain pending at the Commission until further information is provided.

The Final Rule adds a new part to the Commission's regulations, which states that this part applies to all users, owners and operators of the Bulk-Power System within the United States (other than Alaska or Hawaii) and requires that each Reliability Standard identify the subset of users, owners and operators to which that particular Reliability Standard applies. The new regulations also require that each Reliability Standard that is approved by the Commission will be maintained on the ERO's Internet website for public inspection.

The Federal Energy Regulatory Commission has specific instructions on how to enhance the "INT" standards (see the Mandatory Reliability Standards for the Bulk-Power System (issued

March 16, 2007) Docket No. RM06-16-000; Order No. 693). These instructions are captured and included in the attachment. As examples:

FERC Order 693, paragraph 821: Accordingly, the Commission approves Reliability Standard INT-001-2 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to INT-001-2 through its Reliability Standards development process that includes a Requirement that interchange information must be submitted for all point-to-point transfers entirely within a balancing authority area, including all grandfathered and "non-Order No. 888" transfers.

FERC Order 693, paragraph 866: Accordingly, the Commission approves Reliability Standard INT-006-1 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to INT-006-1 through the Reliability Standards development process that: (1) makes it applicable to reliability coordinators and transmission operators and (2) requires reliability coordinators and transmission operators to review energy interchange transactions from the wide-area and local area reliability viewpoints respectively and, where their review indicates a potential detrimental reliability impact, communicate to the sink balancing authorities necessary transaction modifications before implementation.

The Interchange Subcommittee, as custodians of the NERC "INT" standards, will review the FERC Order 693, the NERC 3 Year Standards Work Plan, and the INT-001 and INT-003 through INT-010 standards and initiate SARs as necessary.

Attachment

1. FERC Order 693, Extract for INT Standards
2. NERC Standards 3 Year Plan – Extract for INT Standards

Item 4. E-Tag 1.8

Item 4.a E-Tag 1.8 Implementation Plan Posting — Jim Hansen, Bob Harshbarger

Jim Hansen and Bob Harshbarger will lead the JISWG discussion of the E-Tag Specifications, Schema, Comment Form, and Implementation Plan. In accordance with the E-Tag 1.8 Implementation Plan, the JISWG will respond to vendor comments during this meeting.

Attachments

1. E-Tag 1.8 Project Implementation Plan
2. E-Tag 1.8 Specifications
3. E-Tag 1.8 Schema (The schema will be distributed to the IS, JISWG, and E-Tag Vendor list servers under separate cover due to technical difficulties.)
4. E-Tag 1.8 Comment Form 032307

E-Tag 1.8 Industry Comments to be distributed under separate cover

Item 5. WECC Interchange Milestones

Item 5.a Western Interchange Tool (WIT) Update – Don Lacen

The Western Interchange Tool (WIT) will go into effect on May 1, 2007, or sooner.

WIT has three phases:

Phase I: Electronic tagging

Phase II: Metering, Scheduling, Inadvertent, check-out hourly and at the end of the day

Phase III: Real-time Calculation of ACE Scheduling, One minute real-time validation of net scheduled interchange, One minute net scheduled interchange profiles for AGC utilization (instantaneous and average values of net scheduled interchange)

WIT provides two primary benefits:

1. WIT provides a single source for the net schedules.
2. WIT eliminates net schedule interchange that may be incorrect - allowing two Balancing Authorities to agree to disagree. In the future, WIT will be the authoritative source for net schedule interchange.

Don Lacen will give a WIT update to the subcommittee.

Item 5.b WECC Standards Waivers – Don Lacen

From the FERC Order 693, paragraphs 822 – 825:

c. Regional Difference to INT-001-2 and INT-004-1: WECC Tagging Dynamic Schedules and Inadvertent Payback

822. NERC proposed a regional difference that would exempt WECC from requirements related to tagging dynamic schedules and inadvertent payback. The Commission noted in the NOPR that WECC is developing a tagging requirement for dynamic schedules. The Commission requested information from NERC on the status of the proposed tagging requirement, the time frame for its development, its consistency with INT-001-1 and INT –4-1 and whether the need for an exemption would cease when the tagging requirements become effective. The Commission stated that it would not approve or remand an exemption until NERC submits this information. Rather we stated that we would consider any regional differences contained in a proposed WECC tagging requirement for dynamic schedules when submitted by NERC for Commission review.

823. APPA agrees with the Commission's proposed course of action addressing this regional difference.

824. Xcel requests that the Commission accept the proposed regional difference; tagging requirements for dynamic schedules do not apply now in WECC, and it would be burdensome and would provide little reliability benefit to apply those requirements to WECC by June 2007. The Commission therefore should approve the proposed variance for an interim period until WECC's tagging requirements for dynamic schedules are developed and approved.

ii. Commission Determination

825. The Commission stressed in Order No. 672 that uniformity of Reliability Standards should be the goal and practice, "the rule rather than the exception." The Commission therefore states in the NOPR that the absence of a tagging requirement for dynamic schedules in WECC is a matter of concern, and that for this reason it could not approve or remand this regional difference without the additional information it requested. To date the Commission has not received this information. Of particular importance in this compliance filing will be the ERO's demonstration that this practice is due to a physical difference in the

system or results in a more stringent Reliability Standard. Without this information, we are unable to address Xcel's comments further. The Commission therefore directs the ERO to submit a filing within 90 days of the date of this order either withdrawing this regional difference or providing additional information.

Don Lacen will lead the discussion on not receiving the WECC requested Reliability Standards waivers.

Item 6. IS – ORS Joint Meeting

The Interchange Subcommittee will meet on May 2-3, 2007 with the Operating Reliability Subcommittee to discuss the following three items.

Item 6.a Dynamic Schedule Information in the IDC — Don Lacen, Jim Castle

The Interchange Subcommittee believes that including actual flow data for Dynamic Schedules in the IDC would be a better solution than utilizing average energy forecasts. This information is readily available by participating Balancing Authorities Area Control Error (ACE) equations. In addition, the practice of using average energy forecasts for Dynamic Schedules is very difficult to monitor for compliance purposes. If metered data can be used in the IDC, then the IS will consider changing the standard to require maximum energy values in the E-Tag. This will provide a better reliability solution in forecast hours. The IS requests that the ORS conduct the necessary investigations, utilizing the IDC Working Group if necessary, to determine the feasibility of this approach.

Attachments

Dynamic Schedule Information in the Interchange Distribution Calculator (IDC) Letter from the IS to the ORS, dated March 9, 2007

Item 6.b Reliability Standard INT-006-1 — Don Lacen, Jim Castle

FERC Order 693, paragraph 866: Accordingly, the Commission approves Reliability Standard INT-006-1 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to INT-006-1 through the Reliability Standards development process that: (1) makes it applicable to reliability coordinators and transmission operators and (2) requires reliability coordinators and transmission operators to review energy interchange transactions from the wide-area and local area reliability viewpoints respectively and, where their review indicates a potential detrimental reliability impact, communicate to the sink balancing authorities necessary transaction modifications before implementation.

The IS and ORS will discuss solutions to the FERC Order 693 directive.

Attachments

See FERC Order 693, Extract for INT Standards (found in agenda item 3.b)

Item 6.c Conditional Firm Service — Don Lacen, Jim Castle

On February 16, 2007, the Federal Energy Regulatory Commission (FERC) issued Order Number 890 related to titled “Preventing Undue Discrimination and Preference in Transmission Service.” Order 890 outlines the requirements for providing a transmission product called “conditional firm service.” Conditional firm service would be treated as firm (Firm – Priority 7), except when certain conditions are meant, at which point the transmission service would transition to non-firm (Non-Firm – Priority 6). FERC concludes, at Paragraph 1077 of Order 890, that the provision of conditional firm service will not result in changes to the IDC or to e-tagging.

1077. We disagree with commenters' suggestion that the NERC IDC must be changed to accommodate conditional firm service. We reiterate that we are not creating a new curtailment priority in this Final Rule. We also disagree that new tags that combine a firm and non-firm priority must be developed in order to implement the conditional firm option. The curtailment priority in a tag can be changed ahead of the operating hour based on a near-term forecast of system conditions. We are cognizant that daily and hourly operations to change the tags for conditional firm customers likely involve the need for control room coordination and development of an appropriate tracking process. As the Commission described in the NOPR, new tracking and tagging business practices for this service must be developed by each transmission provider. Thus, we are allowing a sufficient period for the development of these business practices, i.e., 180 days from the date of publication of this Final Rule in the Federal Register. As directed above, transmission providers must coordinate with other transmission providers in their regions to develop these tracking and tagging business practices.

However, EEI's Motion to Extend Certain Order No. 890 Compliance Deadlines for Non-ISO/RTO Transmission Providers and Request for Expedited Treatment states:

B. Specific Software Changes Are Needed to Implement CFS

After reviewing the current software and meeting with vendors, EEI's Non-ISO/RTO TP members believe that the Commission erred when it indicated that the decision to afford CFS the same priority as secondary network service during "conditional periods" could be implemented without fundamental software changes. The Commission correctly recognized that the implementation of CFS would require a change in the priority of a tag from firm (7F) to conditional (i.e., the same as secondary network) (6NN) during a conditional period. But, the Commission claimed that this changing of the tag priority required no software modifications:

> We disagree with commenters' suggestion that the NERC IDC must be changed to accommodate conditional firm service. We reiterate that we are not creating a new curtailment priority in this Final Rule. We also disagree that new tags that combine a firm and non-firm priority must be developed in order to implement the conditional firm option. The curtailment priority in a tag can be changed ahead of the operating hour based on a near-term forecast of system conditions.[fn]
>
> [fn]For example, in the Eastern Interconnection, tags can be changed up to 35 minutes before the hour in which a TLR event is scheduled. *See* NERC Standard IRO-006-3, *Transmission Loading Relief Procedures – Eastern Interconnection*, Section 6.2 (Communications and Timing Requirements) at 23-25 (August 2, 2006).

EEI's Non-ISO/RTO TP members have determined that a Transmission Provider has neither the authority nor the ability to change tags in the manner FERC assumes. The portion of the NERC Standard cited (IRO-006-3 Section 6.2), relates only to the reallocation process during a TLR, not the changing of a tag's priority. This reallocation process that occurs during TLRs is not at all the same as a change to a tag priority. In fact, once submitted, the status (priority) field is may not be edited by anyone.

Indeed, the only existing way to "change" a priority of a tag is to terminate an existing tag altogether and start a new tag. Yet, the approach of terminating an old tag and submitting a new tag would interrupt the flow and cause energy imbalances, unless it could be predicted in advance that the change in priority was necessary, which is not what is envisioned because a "condition" or a determination to use conditional hours could occur while power is flowing. There thus have to be substantial changes made by

OATI to either permit the tag changes required by CFS or develop an alternative solution.
As discussed infra, EEI supports a change in the effective date of CFS for reasons unrelated to this software issue. But, in any case, the effective date for any CFS service agreement should be delayed until the software changes are made, with the requirement that the Transmission Providers exercise due diligence in assuring such changes are made.

Attachments

FERC Order 890, Extract on Conditional Firm Service

Item 7. Future Meetings

Wednesday, September 19, 2007 Thursday, September 20, 2007	8 a.m.–5 p.m. 8 a.m.– noon	Montreal
Wednesday, November 14, 2007 Thursday, November 15, 2007	8 a.m.–5 p.m. 8 a.m.– noon	San Francisco
Wednesday, February 24, 2008 Thursday, February 25, 2008	8 a.m.–5 p.m. 8 a.m.– noon	To Be Determined
Wednesday, May 24, 2008 Thursday, May 25, 2008	8 a.m.–5 p.m. 8 a.m.– noon	To Be Determined
Wednesday, September 24, 2008 Thursday, September 25, 2008	8 a.m.–5 p.m. 8 a.m.– noon	To Be Determined
Wednesday, November 24, 2008 Thursday, November 25, 2008	8 a.m.–5 p.m. 8 a.m.– noon	To Be Determined

Notes:

1. Schedule meetings before the Operating Committee and Planning Committee meetings, whenever possible.
2. Avoid scheduling meetings 30 days before NERC Board of Trustees meetings.
3. Schedule additional meetings, conference calls, or web casts as deemed necessary to address and accomplish subcommittee or task force business.
4. Conduct future Interchange Subcommittee meetings only as necessary: 1) to facilitate necessary face-to-face discussions; 2) to focus on deliverables that cannot be achieved by conference calls or web casts; and 3) to initiate consensus building or decision-making forums.
5. Determine if the Interchange Subcommittee will continue to schedule joint meetings with the NERC-NAESB Joint Interchange Schedule Working Group (JISWG), and with the NERC Operating Reliability Subcommittee (ORS).

Interchange Subcommittee

Chairman	Alan Boesch Operational Compliance Supervisor	Nebraska Public Power District P.O. Box 1000 Doniphan, Nebraska 68832-1000	(402) 845-5210 (402) 845-5238 Fx agboesc@nppd.com
Vice Chairman & WECC	Donald P. Lacen Transmission Services Coordinator	Public Service Company of New Mexico Alvarado Square, MS-EP11 Albuquerque, NM 87158	(505) 241-2032 (505) 241-2582 Fx don.lacen@pnm.com
SERC	John J. Ciza Project Manager	Southern Company Generation 600 North 18th Street Birmingham, Alabama 35291	(205) 257-5879 (205) 257-4441 Fx Jjciza1@southernco.com
FRCC	Ronald L. Donahey Managing Director, Grid Operations	Tampa Electric Co. P.O. Box 111 Tampa, Florida 33601-0111	(813) 623-5120 (813) 630-6299 Fx rldonaey@tecoenergy.com
NPCC	Pat Doran Manager-Market Facilitation	Independent Electricity System Operator Station A Box 4474 Toronto, Ontario M5W 4E5	(905) 855-6233 (905) 855-6249 Fx pat.doran@ieso.ca
RFC	Joe Gardner Director, Real-Time Operations	Midwest ISO, Inc. 701 City Center Drive Carmel, Indiana 46032	(317) 2495446 (317) 249-5910 Fx jgardner@midwestiso.org
SERC	Larry M. Goins Manager, Operations Support	Tennessee Valley Authority 1101 Market Street Chattanooga, Tennessee 37402	(423) 751-7627 (423) 751-3433 Fx lmgoins@tva.gov
WECC	James Michael Hansen Strategic Advisor	Seattle City Light 614 NW 46th Street Seattle, Washington 98107	(206) 706-0165 (206) 706-0183 Fx James.hansen@seattle.gov
RFC	Frederick J. Kunkel Manager transmission Services	Wabash Valley Power Association 722 North High School Road Indianapolis, Indiana 4624-3756	(317) 481-2846 (317) 243-6416 Fx fredk@wvpa.com
SPP	Melinda K. Montgomery Transmission Business Manager, Operations	Entergy Services, Inc. 5201 West Barraque Pine Bluff, Arkansas 71602	(870) 541-4578 (870) 541-3964 Fx Mmontg3@entergy.com
SERC	Michael L. Oatts Manager, EMS Applications	Southern Company Services 14N-8220 P.O. Box 2641 Birmingham, Alabama 35202-2625	(205) 257-7743 (205) 257-5083 Fx mloatts@southernco.com
RFC	Christopher Pacella Analyst-Operations Development	PJM Interconnection, L.L.C 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403	(610) 666-4469 (610) 666-4282 Fx pacelc@pjm.com
WECC	Deanna M. Phillips Senior Electrical Engineer	Bonneville Power Administration Routing PGS P.O. Box 3621 Portland, Oregon 97208	(503) 230-5164 (503) 230-5054 Fx dmphillips@bpa.gov

California ISO **WECC**	Lonnie Rush Manager of Real Time Operations	California ISO 151 Blue Ravine Road Folsom, California 95630	(916) 608-5951 lrush@caiso.com
NPCC	John M. Simonelli Manager Tariff, Schedules & OASIS	ISO New England, Inc. One Sullivan Road Holyoke, Massachusetts 01040-2841	(413) 535-4157 (413) 535-4343 Fx jsimonelli@iso-ne.com
WECC	Robert D. Schwermann Project Manager, System Standards	Sacramento Municipal Utility District 6301 South Street MS A404 Sacramento, California 95817	(916) 732-5519 (916) 732-6436 Fx bschwer@smud.org
Staff Coordinator	Thomas J. Vandervort Reliability Assessment & Performance Analysis Coordinator	North American Electric Reliability Council 116-390 Village Boulevard Princeton, New Jersey 08540-5731	(609) 452-8060 (609) 452-9550 Fx tom.vandervort@nerc.net

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL
Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5721
www.nerc.com • 609-452-8060 (Voice) • 609-452-9550 (Fax)

Interchange Subcommittee (IS) with Joint Interchange Subcommittee Working Group (JISWG)
February 14, 2007

Interchange Subcommittee (IS)
February 15, 2007
San Diego, CA 92130

Draft Minutes

Administration
Vice chair Don Lacen led the welcome and introductions. Bill Lohrman established that a quorum was present for the IS. Bill Lohrman reviewed the NERC Antitrust Compliance Guidelines. Don Lacen reviewed the agenda and the objectives of the meeting.

Attendance
In-person:

Bill Lohrman	Tom Vandervort	Lonnie Rush
Clint Aymond	Jeremy West	David Lemmons
Andy Tritch	Larry Goins	John Ciza
Chris Pacella	John Simonelli	Pat Doron
Don Lacen	Mike Oatts	Jim Hansen
Bob Schwerman	Paul Sorensen	

Via phone:

Ed Overtree	Joe Gardner	Dennis Harrison
Deanna Phillips	Larry Stone	

E-Tagging Functional Specification

Don Lacen led the group in an evaluation of the effectiveness of the December 1st and December 18th conference calls in preparing the industry for E-Tag 1.7.097. The consensus was that there was a pretty good response from PSEs, BAs, and that many more participants than expected joined the call. The callers needed some clarification about how the IS and JISWG is merely implementing the standards that are being approved, and not imposing changes on the industry. In the future it would help if the conference call announcement(s) specifically mention the standards which apply to the changes.

Vice Chairman Don Lacen then led the group in a review the results of the implementation of E-Tag 1.7.097 WECC has submitted an urgent action SAR to modify timing tables, and also submitted a modification request to NAESB regarding INT-006-1 for real time tags with 5 minute assessment period. WECC will have a 10-minute assessment period, vendors have already made the requisite code modifications. The group suggested that WECC contact the NERC Compliance Program and find out what needs to be done to process the urgent action.

The group then discussed the removal of the ability of unilateral cancellation of a transaction. The JISWG is following what is in the standards. Those entities that want to keep unilateral cancellation were counseled to submit a SAR.

Additionally, the group discussed some other E-Tag functionality. When a tag correction comes in, users do not see a reset of the approval window – this will be corrected in Version 1.8 - currently the correction only goes to the entities on the tag. The group suggested that this should probably reset the tag status, and expressed a concern about being restricted to a 3 minute evaluation. The group discussed waiting until version 1.8 or changing spec now, and suggested polling the industry regarding making the change prior to rolling out version 1.8. The group suggested making the change to make the specifications compliant with the standards. The maximum assessment period for reliability purposes may be impacted unless it is adjusted by changing the tag to LATE, only for a tag that hasn't gone implemented prior to the ramp start. Perhaps it should be recommended that correction requests should rejected if they are submitted without enough time to conduct a reliability evaluation based on the ramp start and the total duration of the assessment period as defined in the timing tables. Jeremy West and Jim Hansen will write up a suggested fix to the specification and review it with the e-tag vendors for an evaluation of the feasibility of making the change prior to e-tag 1.8, without a schema change. Will have a conference call with the e-tag vendors and will be based on the requirements of the standard INT-006 and the timing tables.

Jim Hansen led the IS and JISWG in a review of potential updates needed to migrate to version 1.8 of the E-tag specification listed below and reviewed added changes that require schema changes and new definitions:

- Remove Background section
- Add reference to default ramp rate definitions
- Clarify LATE and ATF timelines
- Add new final states and their definitions
    - cancelled, terminated, expired, confirmed, implemented
- Add Rounding definition
- Add Ramp Rate 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 Erroneous Current Level Warning
- Notify entities list (no approval, sent copies of e-Tag)
- Calculation of ActOnByTime
- Addition of TimeClassification
- NERC web site changed to Electric Industry Registry web site
- Add Terminate, Withdraw, DistributeTerminate, and DistributeCancel methods.
- Simplify Recovery function
- Allow ATF e-Tags to be Terminated
- Allow Source or Sink to modify DYNAMIC e-Tag with actual data

The IS will need to add clarification to the Capacity Tag definition, since it is not being used consistently, WECC has issued a regional business practice for two types of capacity products:

1) spin and non-spin 2) interruptible loads

The IS will need to clarify how dynamic e-tags are done; can any entity on the e-tag make an ATF correction to the dynamic schedule? Tom Vandervort will check definitions against NERC Glossary.

The group also discussed the modification to an IMPLEMENTED ATF e-tag through the terminate process ATF and indicated that the E-Tag will need to add feature for E-Tag recovery that automates it rather than requiring provision of each LCA. Single request to authority should recover everything for requestor. Agent should be able to keep list of unique URL's for authority services. Additional changes will be deferred to subsequent updates and the IS will ask industry for suggestions

The IS/JISWG established a preliminary Timeline/Schedule for completing E-Tag 1.8:

- Review by JISWG by Conference Call – February 26th 11-2 Pacific Time
- Completion of draft 1.8 E-tag Specifications – Feb 28th send to E-tag Vendors and IS
- E-tag Vendor conference call Webex March 5th 11 – 1 Eastern time
- Review and approval by IS by Conference Call March 9th 11 – 1 Eastern time
  (both specification and schema)
  Invite JISWG
  Send to E-tag vendors
- Conference call with NERC, NAESB, vendors March 19th 11 – 2 Eastern time
  Develop Project plan
  Training
  Industry conference calls/Workshops (two each WEST and EAST)
  Interoperability Testing
- Post for 30-day industry comment period March 20th
- IS and JISWG reply to comment/ final changes May 2 – 3
  Joint meeting in Portland, OR
- Send to vendors for development May 3
- Vendor development May 5 to Aug 5th
- Industry Webex's t.b.d.
- Interoperabilty vendor testing Aug 5 to Sep 5th
  NERC / NAESB facilitation
  Set up interoperability examples
  Draft site acceptance test plan
- Training / User Testing Sep 5th to Nov 2nd
  4 Workshops t.b.d. in October
  Phoenix/San Diego for West
  Chicago / Atlanta for East
- **Project Implementation – Dec 5th**
- IS Meeting: September 19, 2007 8 a.m.–5 p.m. September 20, 2007 8 a.m.–12 p.m.
  Montreal
- IS Meeting: November 14, 2007 8 a.m.–5 p.m. November 15, 2007 8 a.m.–12 p.m.
  San Francisco, CA – follow ORS

Western Interchange Tool

Don Lacen provided the IS with an update on the Western Interchange Tool. Phase 1 started mid-January and WECC is working on getting all validation errors cleaned up by May 30th. Each BA is working on the validation when PSEs make the tags. By May 30th improper tags no longer be accepted, but it will be easier to create a tag because everything will be standardized with one E-tag Authority. Phase 2 will include metering and inadvertent. Tags will become the schedule because electronic scheduling will be in place, with checkout hourly and at the end of the day. For Phase 3 one minute net scheduled interchange profiles for AGC utilization (instantaneous and average values of net scheduled interchange) will be used.

Interchange Standards

Don Lacen led the IS in a review of the NERC Interchange Standards (INT-001 – INT-010) as part of the subcommittee responsibilities. The IS discussed whether any changes should be made to the scope of the new INT SAR. None were identified. Individual companies can comment as they see fit. INT-004 may need to be revised to be more enforceable related to evaluation of current flow. The IS asked what can the IDC (IDCWG) do related to real time data updates; Mike Oatts will speak with someone at the IDWG. Pat Doran will draft a letter requesting clarification.

The IS then discussed a few questions regarding INT standards that were sent to NERC:
1. INT – 001 The latest word on this standard is that the approval process is changed from tacit approval to tacit denial. That is, previously if an entity responsible for approving or denying a tag did not approve the tag, it was automatically approved. Now, if that entity does not approve a tag, it is denied. Is it a compliance violation for that entity to allow the tag to be denied by not sending a response to the tag request, or is the entity responsible to respond to every tag and either approve or deny?

Yes – INT-006 requires all to be responded to – see Levels of Compliance

2. INT – 004 The issue here is the requirement calling for use of the "average" value for a dynamic schedule tag when that schedule is across a stability limited interface. It appears to open the door for a reliability problem or violation of the interface limit if the entity would use the average value as the requirement calls for. Is it considered to be a compliance violation if the entity observes good reliability practices and uses the MAX value for the dynamic schedule?

Possibly – depends on whether or not M1 is complied with. The JISWG would recommend that the transmission allocation be set to the maximum expected value and that the energy profile be set to the average as required in INT-004. However the average values need to be updated as required in the standard.

3. I have a question concerning reliability standards:
- INT-005 – Interchange Authority Distributes Arranged Interchange
- INT-006 - Response to Interchange Authority
- INT-008 – Interchange Authority Distributes Status

The standards propose to execute the e-tagging process in less than 1 minute. I am referring to Column A of the Timing Table where it states that the Interchange Authority must make an initial distribution of arranged interchange in less than a minute. Current E-tagging process takes 10 to 15 minutes and therefore makes the less then 1 minute requirement unreasonable.

The <1min time in column A refers to the authority service distribution to all entities in the e-tag chain. That is just for the distribution, which is done electronically, and does not refer to the entire e-tag distribution assessment and implementation procedure.

The answers to the above questions were forwarded to the questioners.

Feedback to Vendors on E-Tag 1.7.097

The group provided feedback to vendors on recent changes to E-Tag Specifications. The vendors did a good job of notifying users of change to E-tag 1.7.097.

IS Operating Committee Coverage

Jeremy West provided the IS with a report of the IS issues covered during the last Operating Committee (OC) meeting. Some concerns raised by OC regarding:
- What the standards said about going back to change dynamic tags
- Next business day or 96 hours
- Allowing changes to dynamic tags ATF to get around compliance

Mr. West also described how he relayed Dec 18th conference call information to the OC.

Don Lacen worked with the IS to schedule coverage for upcoming Operating Committee meetings:

March 21 – 22: Long Beach (John Ciza)
- 1.8 plans
- Timing change for assessment period for correction
- IS Work plan

June 6 – 7: Toronto (Pat Doran)
September: t.b.d.
December: t.b.d.

IS Goals for 2007

Don Lacen reviewed the IS goals for the remainder of 2007 and asked that this be a posted, and updated as necessary, on the IS website. The goals for 2007 are:

a. Changes to IDC to use dynamic data rather than the tag
    i. Submit a letter to the IDCWG to make the appropriate changes
        - ICCP or SDX

b. JISWG to issue a SAR to relax approval times for ATF issues for INT and Coordinate
[Has been done]

c. Interchange standards. Need timing table for both standards.
[Has been done]

d. Dynamic Schedule prorata curtailments
   i. Changing the tag does not affect dynamic schedule
      - Currently need to get two BAs to agree to a change on the meter value
      - What needs to be done to fix this situation?
         a. No longer an issue for the IS
   ii. Items in the Dynamic Schedule Reference Document may need to be transferred into a standard
      - Tag adjust may not be sufficient
   iii. Maintaining the dynamic transfer survey
      - Review results and send data to Resources Subcommittee
   iv. Updating dynamic schedule catalog
      - What to do with future planned dynamic schedules
      - What to do with registry [ask Don Benjamin and Tom Vandervort]
   v. Action items
      - Complete review of the catalog
         a. West – Lonnie and Don
         b. East – Mike and Pat and Melinda
      - Develop action plan

e. Continue work on E-tag 1.8 implementation plan (December 5th)
      - Vendor Interoperability
      - User training

f. Getting more market participants to attend IS meetings

g. Draft site acceptance test plan for E-tag 1.8

Review of meeting and posting schedules

The IS established a tentative meeting schedule for 2007. Earlier the IS had indicated a desire to schedule its meetings in conjunction with the ORS. The tentative ORS meeting schedule for 2007 is listed below:

May 2, 2007 8 a.m.–5 p.m.
May 3, 2007 8 a.m.–12 p.m.
Portland, OR Joint with JISWG for both days - follow ORS

September 19, 2007 8 a.m.–5 p.m.
September 20, 2007 8 a.m.–12 p.m.
Montreal

November 14, 2007 8 a.m.–5 p.m.

November 15, 2007 8 a.m.–12 p.m.
San Francisco, CA – follow ORS

The meeting was then adjourned.

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

h

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

E-Tag 1.8 Vendors Meeting

E-Tag 1.8 Vendors - Specifications and Schema Technical Review

Friday, March 16, 2007
Salt Lake City, Utah

Minutes

Administrative

Jim Hansen, JISWG co-chair , led the welcome and introductions. Tom Vandervort reviewed the NERC Antitrust Compliance Guidelines\

Attendance

In-person:

Bob Winn – OATI
Brian Lewis – OATI
Joe Buttress – OATI
Nelson Mueller – OATI
Jim Hansen – Seattle City Light
Bill Lohrman – NERC Consultant

Phone:

DeDe Kirby – NAESB
Don Lacen – PNM
Phillip Shafeei – NYISO
Carla Dantzler – Sungard
Patrick Cromer – MCG
Clint Aymond – Entergy
Tom Vandervort – NERC
Ed Overtree – NAESB
Andy Tritch – Sungard
Larry Stone – SoftSmiths
Jeremy West – Entergy

E-Tag 1.8 Technical Review

Brian Lewis and Jim Hansen led a review of the Vendor E-Tag 1.8 technical specifications and schema. During the meeting the group discussed modifications made to the specifications (**Exhibit A**) and schema (**Exhibit B**).

During the discussion, the group developed two questions that would be included as part of the comment form during the posting period:

1. How should MW hourly/daily rounding be handled?
2. What should be displayed?

The E-tag vendors were asked to develop examples regarding the implementation of potential changes for periodicity.

The group discussed the need for accommodating recently approved Western Electric Coordinating Council in the specifications and schema. Brian Lewis volunteered to develop a

separate specifications document for that purpose that would be separate from the main E-Tag 1.8

Future Meetings / Conference Calls

The next conference call was confirmed for Monday, March 19, 2007, 11 a.m. – 2 p.m., EST. The purpose of the call will be to develop project plan to complete the remaining tasks for finishing E-Tag 1.8.

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interchange Subcommittee
May 2, 2007 Meeting
Open Action Item List

Action Figure	Subject	Action Item/Assignment	Due Date	Completion Date
Tom Vandervort	Dynamic Schedule In IDC Letter to ORS	021507, Tom Vandervort to send IS letter to ORS regarding the "Dynamic Schedule Information in the Interchange Distribution Calculator (IDC). 030907, Letter sent to ORS	030907	030907
Don Lacen	2007 IS Goals	010107, Don Lacen reviewed the IS goals for the remainder of 2007 and asked that this be a posted, and updated as necessary, on the IS website. The goals for 2007 are: a. Changes to IDC to use dynamic data rather than the tag i. Submit a letter to the IDCWG to make the appropriate changes • ICCP or SDX b. JISWG to issue a SAR to relax approval times for ATF issues for INT and Coordinate c. Interchange standards. Need timing table for both standards. d. Dynamic Schedule pro-rata curtailments i. Changing the tag does not affect dynamic schedule • Currently need to get two BAs to agree to a change on the meter value • What needs to be done to fix this situation? a. No longer an issue for the IS ii. Items in the Dynamic Schedule Reference Document may need to be transferred into a standard • Tag adjust may not be sufficient	a. b. 033007 c. 033007 d.	a. b. 033007 c. 033007 d.

Action Figure	Subject	Action Item/Assignment	Due Date	Completion Date
		iii. Maintaining the dynamic transfer survey ● Review results and send data to Resources Subcommittee iv. Updating dynamic schedule catalog ● What to do with future planned dynamic schedules ● What to do with registry [ask Don Benjamin and Tom Vandervort] v. Dynamic schedule action items ● Complete review of the catalog a. West – Lonnie and Don b. East – Mike, Pat and Melinda ● Develop action plan e. Continue work on E-tag 1.8 implementation plan (December 5th) ● Vendor Interoperability ● User training f. Getting more market participants to attend IS meetings g. Draft site acceptance test plan for E-tag 1.8	e. f. g.	e. f. g.
Jim Hansen and Bob Harshbarger	E-Tag version 1.8	032307, The Interchange Subcommittee will implement the E-Tag, version 1.8 implementation plan: Notes: 1) The dates are tentative and subject to change, depending on obstacles encountered during the implementation of the project plan. 2) Additional meetings, conference calls/webcasts, workshops may be scheduled to support the project plan. 050207, In progress	123107	
		E-Tag, version 1.8 implementation plan: E-Tag 1.8 Project Implementation Plan posted for 30 day comment period (March 20 – April 20, 2007)	032007	032007
		E-Tag, version 1.8 implementation plan: Develop and Post Responses to Industry Comments on NERC and NAESB web	050307	

Action Figure	Subject	Action Item/Assignment	Due Date	Completion Date
		sites (IS and JISWG Generate Responses and Incorporate Changes to the Final Plan)		
		E-Tag, version 1.8 implementation plan: E-Tag, version 1.8 Vendor Development (May 3 – August 5, 2007)	080507	
		E-Tag, version 1.8 implementation plan: IS and JISWG to Create Industry Tutorial / Q&A / Information Sharing Coordinated Webcasts	To Be Determined	
		E-Tag, version 1.8 implementation plan: Interoperability Vendor Testing, August 5 – September 5, 2007 • NERC / NAESB Facilitation • Set-up Interoperability Examples • Draft site acceptance test plan • Etc. Details to be worked out	090507	
		E-Tag, version 1.8 implementation plan: Industry Training / User testing / Workshops (tentatively schedule 4 workshops) / (September 5 – November 2, 2007)	110207	
Jim Hansen	E-Tag 1.9.097 Reliability Assessment Timing Violations	030507, During the March 5, NERC/NAESB JISWG conference call, the JISWG and E-Tag Vendors agreed to reset the reliability assessment timer on the Authority based on the time the Authority receives the correction request for e-Tags with a composite state of PENDING to the full reliability assessment period defined in the NERC/NAESB Coordinate Interchange timing table. The correction request must be marked as LATE as appropriate by the Authority Service. In this case, the Authority must reset all approval states for all entities to PENDING. A letter was sent on March 5, 2007 to E-Tag vendors addressing this change to be implemented on April 4th, 2007 15:00 Central Daylight Time.	040407	
Mike Oatts	IDC Real-time Data Updates	021507, Mike Oatts to discuss with someone on the IDCWG regarding what can IDC (IDCWG) do related to real-time data updates.	050207	

Action Figure	Subject	Action Item/Assignment	Due Date	Completion Date
John Ciza	OC Presentation	021507, John Ciza to present the E-Tag 1.8 status to the NERC Operating Committee in Long Beach, on March 21-22, 2007.	032207	032207

6. INT: Interchange Scheduling and Coordination

795. The Interchange Scheduling and Coordination (INT) group of Reliability Standards addresses interchange transactions,[278] which occur when electricity is transmitted from a seller to a buyer across the power grid. Specific information regarding

[276] See supra P 779.

[277] Order No. 890 at P 196.

[278] The NERC glossary defines "interchange" as "Energy transfers that cross Balancing Authority boundaries." NERC Glossary at 9.

each transaction must be identified in an accompanying electronic label, known as a "Tag" or "e-Tag" which is used by affected reliability coordinators, transmission service providers and balancing authorities to assess the transaction for reliability impacts. Communication, submission, assessment and approval of a Tag must be completed for reliability consideration before implementation of the transaction.

a. Interchange Authority

796. The Version 1 INT Reliability Standards submitted with NERC's August 28, 2006 supplemental filing include a new entity, the interchange authority, which oversees interchange transactions and is included as an applicable entity or referenced in the Requirements sections of INT-005-1, INT-006-1, INT-007-1, INT-008-1, INT-009-1 and INT-010-1.[279] The Commission requested in the NOPR that NERC provide additional information regarding the role of the interchange authority so that the Commission could determine whether the interchange authority is a user, owner or operator of the Bulk-Power System required to comply with mandatory Reliability Standards.

i. Comments

797. ISO-NE states that it is unclear who the interchange authority should be, how its tasks could be performed operationally and how the interchange authority function relates to other reliability and market functions. ISO-NE states that NERC has not yet fully incorporated the concept of an interchange authority into its Functional Model and has not provided a means for an entity to register as an interchange authority under the

Functional Model. Finally, ISO-NE states that NERC must still create a process to allow the appropriate entities to register as interchange authorities so that their status is clear to all applicable entities, and it urges that approval of the Reliability Standards that have the interchange authority as an applicable entity be withheld until these issues are resolved.

798. APPA agrees that applicability of the Reliability Standards to the interchange authority is confusing. However, APPA suggests the best approach to the problem is for NERC to identify the source and sink balancing authorities as the applicable entity in these Reliability Standards until the Functional Model is revised to better specify the status and responsibility of interchange authorities.

[279] The NERC Glossary defines an "interchange authority" as "the responsible entity that authorizes implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes." Id.

799. EEI observes that there is considerable confusion throughout the industry regarding the registration process and the relationship between registration and applicability of standards, with the interchange authority being an example of that confusion. However, EEI states it understands that the role of an interchange authority is currently being addressed and revisions to the Functional Model are currently moving through the approval process. If Version 3 of the Functional Model is approved by the NERC Board, EEI believes it will clarify that a sink balancing authority performing a Tag authority service could serve as an interchange authority and this modification would address the Commission's concern.

800. The CAISO suggests that it is premature to place any INT Reliability Standards involving an interchange authority into effect until more information is provided concerning the interchange authority's role.

ii. Commission Determination

801. The NERC glossary definition of interchange authority indicates that it is intended

to provide essentially a quality control function in verifying and approving interchange schedules and communicating that information. Our understanding is that, in the interim, sink and source balancing authorities will serve as interchange authorities until the ERO has further clarified an interchange authority's role and responsibility in the modification of the Functional Model and in the registration process. The new interchange authority function allows an entity other than a balancing authority to perform this function in the future; the pre-existing INT-001-1 Reliability Standard identified the balancing authority as the responsible entity to perform this function. Any such entity should be registered by the ERO in the ERO compliance registry, so that the responsibility of an entity, other than a balancing authority, that takes on this role in the future would be clear.

802. In short, there is sufficient clarity concerning the nature and responsibilities of this function for it to be implemented at this time. Withholding approval of INT Reliability Standards pending further clarification on this matter would create an unnecessary gap in the coverage of the Reliability Standards that potentially could threaten the reliability of the Bulk-Power System.

b. Interchange Information (INT-001-2)

803. INT-001-1 seeks to ensure that interchange information is submitted to the reliability analysis service identified by NERC.[280] This Reliability Standard applies to

[280] Currently, the reliability analysis service used by NERC is the Interchange Distribution Calculator.

purchasing-selling entities and balancing authorities. It specifies two Requirements that focus primarily on establishing who has responsibility in various situations for submitting the interchange information, previously known as transaction tag data, to the reliability analysis service identified by NERC. The Requirements apply to all dynamic schedules,

delivery from a jointly owned generator and bilateral inadvertent interchange payback.

804. The Commission proposed in the NOPR to approve Reliability Standard INT-001-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of its regulations, the Commission proposed to direct NERC to submit a modification to INT-001-1 that: (1) includes Measures and Levels of Non-Compliance and (2) includes a Requirement that interchange information must be submitted for all point-to-point transfers entirely within a balancing authority area, including all grandfathered and "non-Order No. 888" transfers.[281]

805. The Commission also noted in the NOPR that certain Requirements of INT-001-0 that relate to the timing and content of e-Tags had been deleted in the Version 1 Reliability Standard. NERC indicated that these Requirements are business practices that would be included in the next version of the NAESB Business Practices. The Commission stated in the NOPR that NERC's explanation of this change was acceptable and proposed to approve INT-001-1 with the deletion of Requirements R1.1, R3, R4 and R5. However, the Commission also noted that NAESB had not yet filed the e-Tagging requirements as part of its business practices, and that if no such business practice has been submitted at the time of the Final Rule, the Commission may reinstate these Requirements in the Final Rule.

806. NERC submitted INT-001-2, which supersedes the Version 1 Reliability Standards, in its November 15, 2006 filing. INT-001-2 adds Measures and Levels of Non-Compliance to the Version 0 Reliability Standard. In this Final Rule, the Commission addresses INT-001-2, as filed with the Commission on November 15, 2006.

i. Comments

807. APPA states that NERC's submission of INT-001-2 on November 15, 2006 has fulfilled the Commission's proposed directive to include Measures and Levels of Non-Compliance in this Reliability Standard. APPA also states that, while it does not oppose

NERC consideration of the Commission's proposed directive regarding the submission of
interchange information for all point-to-point transfers entirely within a balancing
[281] This Requirement was included in INT-001-0 as Requirement R1.2.

authority area, it does not understand the Commission's reliability concerns in this connection.

808. MidAmerican states that it favors the Commission's proposed directive to NERC
for a modification of the Reliability Standard as a substantial improvement for reliability.

Constellation supports this proposal and states that the proposal, together with other
initiatives, such as OATT reform, represent additional steps to achieving not only Bulk-
Power System reliability, but also a reduction of undue discrimination in transmission
services.

809. NERC disagrees with the Commission's proposal to direct the submission of interchange information on all point-to-point transfers within a balancing area. NERC
contends that this issue was discussed at great length in the Reliability Standards development process and the vast majority of commenters and voters agreed that such a
requirement would have no merit from a reliability perspective. It also states that such
data is not used today by the NERC interchange distribution calculator for reliability.[282]

Finally, NERC concludes that while it may be appropriate for this issue to be reconsidered in revisions to the Reliability Standards, a Commission directive to include
a requirement that the collective expertise and the consensus of the industry have determined to be unnecessary for reliability constitutes "setting the standard."

810. LPPC agrees with the Commission that Requirements R1.1, R3, R4 and R5 are
good business practices, and it states that for this reason they should not be included in
the Reliability Standards. These business practices should more appropriately be contained in NAESB standards, or perhaps the pro forma OATT.

811. ERCOT maintains that INT-001-1 is not appropriate for the ERCOT region. ERCOT states that it is a single balancing authority. To the extent that INT-001-1 requires tagging transfers within a single balancing authority, it cannot be applied to

ERCOT as written because all point-to-point transfers within ERCOT are financial transactions only. ERCOT notes that it tags transfers outside the ERCOT region.

812. Allegheny states that the requirement to tag point-to-point transactions cannot be met in the PJM market where Tags are not used when a transaction's source and sink are

[282] The NERC glossary defines the interchange distribution calculator as "[t]he mechanism used by Reliability Coordinators in the Eastern Interconnection to calculate the distribution of Interchange Transactions over specific Flowgates. It includes a database of all Interchange Transactions and a matrix of the Distribution Factors for the Eastern Interconnection." NERC Glossary at 9.

within the PJM footprint. Such transactions are reported through the PJM eSchedule system, which already provides adequate information for the PJM region to conduct reliability and curtailment analyses. Allegheny states that there is no reliability gap in the PJM market arising from this issue.

813. Santa Clara submits that LSEs should be applicable entities under proposed revised INT-001-2 to ensure that they have adequate notice of the requirements of this Reliability Standard. It states that the actions of LSEs are implicated in Requirement R1 of this proposed Reliability Standard.[283]

ii. Commission Determination

814. The Commission approves INT-001-2 as a mandatory and enforceable Reliability Standard. In addition, we direct the ERO to develop modifications to the Reliability Standard through the Reliability Standards development process, as discussed below.

815. We agree with APPA that INT-001-2, submitted on November 15, 2006 includes Measures and Levels of Compliance, and we will not direct any further action regarding Measures and Levels of Compliance at this time.

816. MidAmerican and Constellation support the Commission's proposal that this Reliability Standard include a Requirement that interchange information must be submitted for all point-to-point transfers entirely within a balancing authority area,

including all grandfathered and "non-Order No. 888" transfers. The Commission points out that unless these grandfathered and "non-Order No. 888" transfers are included in one of the INT Reliability Standards, they might not be subject to appropriate curtailment as necessary due to system conditions. Curtailments are determined using the interchange distribution calculator. Unless transactions internal to a balancing authority area are included in the calculator as we proposed, they are not recognized by the calculator and may never be curtailed. For instance, even if a transaction internal to a balancing authority area is non-firm and some inter-balancing authority trades are firm, the latter could be cut before the former, despite the curtailment priorities in the Order No. 888 tariff. While we recognize that most trades internal to a balancing authority area do not affect interchange, some do, since electricity flows do not necessarily follow the contract path.

283 INT-001-2 Requirement R1 provides that the LSE and purchasing-selling entity shall ensure that arranged interchange is submitted to the interchange authority.

817. In addition, e-Tagging of such transfers was previously included in INT-001-0 and the Commission is aware that such transfers are included in the e-Tagging logs. In short, the practice already exists, but if this Requirement is removed from INT-001-2, no Reliability Standard would require that such information be provided. We therefore will adopt the directive we proposed in the NOPR and direct the ERO to include a modification to INT-001-2 that includes a Requirement that interchange information must be submitted for all point-to-point transfers entirely within a balancing authority area, including all grandfathered and "non-Order No. 888" transfers.

818. The Commission agrees with ERCOT's conclusion that the Reliability Standard does not apply to financial point-to-point transfers within the ERCOT region. This interpretation is consistent with the proposed INT Reliability Standards. Likewise,

Allegheny's views on tagging point-to-point transactions within the PJM market are consistent with the proposed INT Reliability Standards.

819. With respect to Santa Clara's position that LSEs should be applicable entities under the Reliability Standard, the Commission notes that in situations where a LSE is securing energy from outside the balancing authority to supply its end-use customers, it would function as a purchasing-selling entity, as defined in the NERC glossary, and would be included in the NERC registry on that basis. This interpretation flows from the language of the Reliability Standards, and the Commission does not perceive any ambiguity in this connection. Nevertheless, the Commission directs the ERO to consider Santa Clara's comments, and whether some more explicit language would be useful, in the course of modifying INT-001-2 through the Reliability Standards development process.

820. The Commission accepts NERC's explanation that Requirements R1.1, R3, R4 and R5 of INT-001-0 that were deleted in INT-001-1 are business practices. NAESB voluntarily filed "Standards for Business Practices and Communication Protocols for Public Utilities" in Docket No. RM05-5-000 on November 16, 2006. This filing contains wholesales electric business practice standards that incorporate e-Tagging requirements and is the subject of a separate rulemaking process that is expected to result in rules that will become effective on or about the same time as the Reliability Standard becomes mandatory.

821. Accordingly, the Commission approves Reliability Standard INT-001-2 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to INT-001-2 through its Reliability Standards development process that includes a Requirement that interchange information must be submitted for all point-toDocket

point transfers entirely within a balancing authority area, including all grandfathered and
"non-Order No. 888" transfers.[284]

c. Regional Difference to INT-001-2 and INT-004-1: WECC Tagging Dynamic Schedules and Inadvertent Payback

822. NERC proposed a regional difference that would exempt WECC from requirements related to tagging dynamic schedules and inadvertent payback. The Commission noted in the NOPR that WECC is developing a tagging requirement for
dynamic schedules. The Commission requested information from NERC on the status of
the proposed tagging requirement, the time frame for its development, its consistency
with INT-001-1 and INT-004-1 and whether the need for an exemption would cease
when the tagging requirements become effective. The Commission stated that it would
not approve or remand an exemption until NERC submits this information.[285] Rather, we
stated that we would consider any regional differences contained in a proposed WECC
tagging requirement for dynamic schedules when submitted by NERC for Commission
review.

i. Comments

823. APPA agrees with the Commission's proposed course of action addressing this
regional difference.

824. Xcel requests that the Commission accept the proposed regional difference; tagging requirements for dynamic schedules do not apply now in WECC, and it would be
burdensome and would provide little reliability benefit to apply those requirements to
WECC by June 2007. The Commission therefore should approve the proposed variance
for an interim period until WECC's tagging requirements for dynamic schedules are
developed and approved.

ii. Commission Determination

825. The Commission stressed in Order No. 672 that uniformity of Reliability Standards should be the goal and practice, "the rule rather than the exception."[286] The

Commission therefore stated in the NOPR that the absence of a tagging requirement for

[284] The Requirement was included in INT-001-0 as Requirement R1.2.

[285] To date, the Commission has not received the requested information.

[286] Order No. 672 at P 290.

dynamic schedules in WECC is a matter of concern, and that for this reason it could not approve or remand this regional difference without the additional information it requested. To date the Commission has not received this information. Of particular importance in this compliance filing will be the ERO's demonstration that this practice is due to a physical difference in the system or results in a more stringent Reliability Standard. Without this information, we are unable to address Xcel's comments further.

The Commission therefore directs the ERO to submit a filing within 90 days of the date of this order either withdrawing this regional difference or providing additional information.

d. Regional Difference to INT-001-2 and INT-003-2: MISO Energy Flow Information

826. NERC proposed a regional difference that would allow MISO to provide market flow information in lieu of tagging intra-market flows among its member balancing authorities; the MISO energy flow information waiver is needed to realize the benefits of locational marginal pricing within MISO while increasing the level of granularity of information provided to the NERC TLR Process. The waiver request text states that it is understood that the level of granularity of information provided to reliability coordinators must not be reduced or reliability will be negatively affected. The waiver request text includes a condition specifying that the "Midwest ISO must provide equivalent information to Reliability Authorities as would be extracted from a transaction tag." The Commission proposed in the NOPR to approve this regional difference. It explained there that, based on the information provided by NERC, the proposed regional difference

is necessary to accommodate MISO's Commission-approved, multi-control area energy market. Thus, the Commission stated it believed that the regional difference is appropriate, because it is more stringent than the continent-wide Reliability Standard and otherwise satisfies the statutory standard for approval of a Reliability Standard.

i. Comments

827. APPA agrees with Commission's proposed course of action in approving this regional difference.

ii. Commission Determination

828. The information received by the Commission demonstrates that the proposed regional difference to INT-001-2 and INT-003-2, as filed on November 15, 2006, is necessary to accommodate MISO's Commission-approved, multi-control area energy market. The Commission concludes that the regional difference is appropriate, because it is more stringent than the continent-wide Reliability Standard and otherwise satisfies the

statutory standard for approval of a Reliability Standard, and therefore approves it as mandatory and enforceable.

e. Interchange Transaction Implementation (INT-003-2)

829. The purpose of INT-003-1 is to ensure that balancing authorities confirm interchange schedules with adjacent balancing authorities before implementing the schedules in their area control error equations. INT-003-1 contains a Requirement that focuses on ensuring that a sending balancing authority confirms interchange schedules with its receiving balancing authority before implementing the schedules in its control area. The proposed Reliability Standard also requires that, for the instances where a high voltage direct current (HVDC) tie is on the scheduling path, both sending and receiving balancing authorities have to coordinate with the operator of the HVDC tie.

830. The Commission proposed in the NOPR to approve Reliability Standard INT-003-1 as mandatory and enforceable. In addition the Commission proposed to direct NERC to submit a modification to INT-003-1 that includes Measures and Levels of Non-Compliance.

831. NERC filed INT-003-2 with the Commission on November 15, 2006. This Reliability Standard supersedes the Version 1 Reliability Standard INT-003-1 and adds
Measures and Levels of Non-Compliance.

i. Comments

832. APPA states that INT-003-2 fulfils the Commission's proposed directive to include Measures and Levels of Non-Compliance.

ii. Commission Determination

833. INT-003-1 serves an important purpose in requiring receiving and sending balancing authorities to confirm and agree on interchange schedules. With the addition
of Measures and Levels of Non-Compliance, INT-003-2 addresses the Commission's
only reservation regarding this Reliability Standard. Accordingly, the Commission approves Reliability Standard INT-003-2, as filed with the Commission on November 15,
2006, as mandatory and enforceable.

f. Regional Differences to INT-003-2: MISO/SPP Scheduling Agent and MISO Enhanced Scheduling Agent

834. NERC proposed a regional difference that would provide MISO and SPP with a
variance from INT-003-1 to permit a market participant to use a scheduling agent to
prepare a transaction Tag on its behalf.[287] In addition, NERC proposed the MISO Enhanced Scheduling Agent Waiver, whichcreates a variance from INT-003-1 for MISO
that permits an enhanced single point of contact scheduling agent.

835. The Commission proposed in the NOPR to approve these two additional regional
differences. The Commission explained that, based on the information provided by NERC, the proposed regional differences for this INT Reliability Standard would provide
administrative efficiency, and provide equal or greater amounts of information to the
appropriate entities as required in MISO's Commission-approved multi-control area
energy market. The NOPR stated that the regional difference is appropriate because it is
more stringent than the continent-wide Reliability Standard and otherwise satisfies the
statutory standard for approval of a Reliability Standard.

i. Comments

836. APPA agrees with the Commission's proposed approval of these regional differences.

837. FirstEnergy states that it would be helpful if NERC clarified the function and effect of these waivers. FirstEnergy states that, where a specific task will be performed by another entity on behalf of the transferor, the transferor entity needs a delegation agreement, whereas in transferring a responsibility, the transferor entity needs a waiver. FirstEnergy states that currently balancing authorities are held accountable by regional reliability organizations for those functions the waivers transfer to the regional reliability organization. FirstEnergy suggests that NERC should clarify that, under these waivers, responsibility for complying with these Reliability Standards should be transferred to the RTOs that actually perform the tasks associated with these requirements.

[287] NERC proposed three regional differences for INT-003-1 that would apply to MISO. One proposed regional difference was addressed in Reliability Standard INT-001-1. The remaining two are discussed here.

ii. Commission Determination

838. These two variances from INT-003-2, as filed with the Commission on November 15, 2006, permit a market participant to use a scheduling agent to prepare a transaction tag on its behalf, providing administrative efficiency and providing equal or greater amounts of information to the appropriate entities as required in MISO's Commissionapproved multi-control area energy market. This regional difference is appropriate because it is more stringent than the continent-wide Reliability Standard and otherwise satisfies the statutory standard for approval of a Reliability Standard. The Commission therefore approves the MISO/SPP Scheduling Agent Waiver and the MISO Enhanced Scheduling Agent Waiver as mandatory and enforceable regional differences to INT-003-2.

839. FirstEnergy may raise its suggestions in the Reliability Standards development process. However, we find that FirstEnergy's suggestion does not affect our decision to approve these two regional differences.

g. Dynamic Interchange Transaction Modifications (INT-004-1)

840. INT-004-1 seeks to ensure that dynamic transfers are adequately tagged to be able to determine their reliability impact. It requires the sink balancing authority, i.e., the balancing authority responsible for the area where the load or end-user is located, to communicate any change in the transaction. It also requires the updating of Tags for dynamic schedules.

841. In the NOPR, the Commission proposed to approve Reliability Standard INT-004-1 as mandatory and enforceable. The Commission also proposed to direct NERC to submit a modification to INT-004-1 that includes Levels of Non-Compliance.

i. Comments

842. APPA agrees with the Commission that INT-004-1 can be approved as a mandatory and enforceable Reliability Standard. However, it suggests that the missing Levels of Non-Compliance should be developed and submitted for Commission approval before penalties are levied for violations.

ii. Commission Determination

843. As explained in the NOPR, while the Commission has identified concerns with regard to INT-004-1, this proposed Reliability Standard serves an important purpose by setting thresholds on changes in dynamic schedules for which modified interchange data must be submitted. Further, the Requirements set forth in INT-004-1 are sufficiently

clear and objective to provide guidance for compliance. Accordingly, the Commission approves Reliability Standard INT-004-1 as mandatory and enforceable. In addition, the

Commission directs the ERO to consider adding these Measures and Levels of Non-
Compliance to the Reliability Standard.

h. Interchange Authority Distributes Arranged Interchange (INT-005-1)

844. INT-005-1 seeks to ensure the implementation of interchange between source and sink balancing authorities and that interchange information is distributed by an interchange authority to the relevant entities for reliability assessments.

845. The Commission proposed in the NOPR to approve Reliability Standard INT-005-1 as mandatory and enforceable. The Commission also proposed to direct NERC to submit a modification to INT-005-1 that includes Levels of Non-Compliance. Further, the Commission noted that INT-005-1 is applicable to the "interchange authority" and requested that NERC provide additional information regarding the role of the interchange authority so that the Commission can determine whether it is a user, owner or operator of the Bulk-Power System that is required to comply with mandatory Reliability Standards.

i. Comments

846. Comments on the interchange authority have been discussed above under the heading "INT Reliability Standards General Issues." No other comments on INT-005-1 have been submitted.

ii. Commission Determination

847. The Commission has set forth above its analysis and conclusion on interchange authorities. Our understanding is that, in the interim, source and sink balancing authorities will serve as interchange authorities until the ERO has clarified the role and responsibility of an interchange authority in the modification of the Functional Model and in the registration process.

848. The Commission is satisfied that the Requirements of INT-005-1 are appropriate to ensure that interchange information is distributed timely and available for reliability assessment. Accordingly, the Commission approves Reliability Standard INT-005-1 as

mandatory and enforceable. In addition, the Commission directs the ERO to consider
adding additional Measures and Levels of Non-Compliance to the Reliability Standard.

i. Response to Interchange Authority (INT-006-1)

849. INT-006-1 applies to balancing authorities and transmission service providers, and
requires these entities to evaluate the energy profile and ramp rate of generation that
supports interchange transactions in response to a request from an interchange authority
to change the status of an interchange from an arranged interchange transaction to a
confirmed interchange.

850. The Commission proposed in the NOPR to approve Reliability Standard INT-006-
1 as mandatory and enforceable. In addition, the Commission proposed to direct NERC
to submit a modification to INT-006-1 that: (1) makes it applicable to reliability
coordinators and transmission operators and (2) requires reliability coordinators and
transmission operators to review composite transactions from the wide-area reliability
viewpoint and, where their review indicates a potential detrimental reliability impact,
communicate to the sink balancing authorities necessary transaction modifications before
implementation.

i. Comments

851. APPA agrees that INT-006-1 is sufficient for approval as a mandatory and enforceable reliability standard. However, APPA states that the Commission should
merely instruct NERC to respond to the Commission's concerns and refrain from directing NERC to make specific changes to the Reliability Standard; APPA states that
while the changes the Commission proposes may be appropriate, it should be left to
NERC's expertise and the Reliability Standards development process to address the
Commission's concerns.

852. FirstEnergy agrees that it is appropriate for the reliability coordinator to be

included in the applicability section. However, it argues that it is impracticable in large organized markets, such as those of MISO and PJM, for a local entity, such as a transmission operator, to review wide-area transactions, and it does not improve reliability to do so. Transactions occurring totally within the market operation are provided as part of network service net scheduled interchange.

853. EEI states that the "wide-area reliability impact" review envisioned by the Commission, which involves review of the composite energy interchange transactions, probably already takes place under Reliability Standards INT-005 through INT-009 in a cost-effective manner. EEI explains that since most transactions submitted by wholesale markets to the transactions tagging process span multiple hours with varying sizes (in MW), and are often submitted days before transaction start times, the wide-area review consists of ensuring that sufficient generator ramping capability exists, as well as examining for limits on transfer capabilities. This review is generally considered

sufficient to the extent that analyses are taking place on the basis of projected system conditions. EEI suggests that the Commission-proposed review and validation of composite energy interchange transactions by reliability coordinators might be more effectively addressed through "near real-time" system review. It explains that, at this time, the broad range of system condition parameters is better known, and the reliability coordinators can make use of the TLR process to maintain system reliability.

854. Entergy disagrees with the Commission's proposed modifications. It contends that they will require substantial changes to the tagging specifications. Entergy believes that the Commission's concerns may already be addressed by Reliability Standards INT-005 through INT-009.

855. MISO believes the Reliability Standards and e-Tag specifications already require reliability entities to evaluate and approve e-Tags. It questions the value of specifying reliability coordinators and transmission operators as applicable entities because their

responsibilities are already laid out in the Reliability Standards.

856. Northern Indiana contends that the NOPR's discussion of INT-006-1 is unclear and confusing. It states that it does not understand what the Commission means by "validate" when the Commission proposes that reliability coordinators and transmission operators review and validate composite arranged interchanges. Northern Indiana also questions whether both reliability coordinators and transmission operators would be required to validate and approve the Tags and what the basis for approval would be. It questions what falls within the term "potential detrimental reliability impact," what happens if a Tag is not validated within 20 minutes to the hour, and whether all schedules are canceled outright or passively approved.

857. TVA suggests that the term "composite Tag" should be defined as part of the proposed modifications. CAISO also questions the meaning of "composite Tag" and seeks clarification on that issue. TVA notes that depending on the type of reliability analysis required to validate a "composite Tag," it may prove impractical to conduct this evaluation for hourly transactions.

858. CAISO states that neither NERC nor the Commission has identified a deficiency in the current interchange reliability assessment process or a pressing reliability need for this Reliability Standard. CAISO also has concerns about meeting the Commissionproposed directives regarding INT-006-1 since reliability coordinators and transmission operators within the Western Interconnection currently do not have a common database from which to draw the information needed to review composite transactions from a wide-area reliability viewpoint. CAISO requests the Commission to consider whether the Western Interconnection should comply with these proposed Requirements at all or whether a transition period is appropriate.

ii. Commission Determination

859. The Commission approves INT-006-1 as mandatory and enforceable. In addition, we direct that NERC develop modifications to the Reliability Standard, as discussed below.

860. The Commission remains convinced that a proactive approach is superior to a reactive approach in maintaining system reliability. While EEI and Entergy claim that reliability coordinators and transmission operators' involvement in reliability reviews of interchange transactions are covered in INT-005 through INT-010, and MISO claims that such review is covered in other Reliability Standards, we note the following: References to reliability coordinator and transmission operator involvement are virtually absent from the INT Reliability Standards. One finds such references only in Requirement R2 of INT-010, which deals with interchange coordination exemptions, and there the involvement of reliability coordinators is restricted to situations that involve current or imminent reliability-related reasons for action. We cannot find any Requirements in the remaining INT Reliability Standards that require a wide-area reliability assessment, regardless of the time periods, by a reliability coordinator; wide-area reliability assessment, moreover, can only be carried out by reliability coordinators.

861. With respect to MISO's comment on the value of applying the Reliability Standard to reliability coordinators and transmission operators given that the Reliability Standards and the e-Tag specification already require evaluation and active approval of reliability entities on e-Tags, we note that none of the INT Reliability Standards have those requirements and that the e-Tag specification is not part of the mandatory Reliability Standards. Like reliability coordinators who are responsible for reliable operation of entire reliability coordinator areas, a transmission operator is the reliability entity responsible for its local area operations. Interchange transactions would be likely to reduce system reliability if those transactions are not reviewed and approved by the appropriate reliability entities before implementation.

862. With respect to the question raised by TVA and CAISO on the definition of "composite Tags," we expressed our reliability concerns in the NOPR and explained that reliability coordinators and transmission operators should review composite energy interchange transaction information (composite Tags) for wide-area reliability impact. In addition, we stated that when the review indicated a potential detrimental reliability impact, the reliability coordinator or transmission operator should communicate to the sink balancing authority the necessary transaction modifications before

implementation.[288] While we did not require a specific notification time prior to actual transactions, this proactive approach should promote system reliability.

863. We agree with FirstEnergy that it is appropriate to include reliability coordinators as applicable entities for purposes of conducting wide-area reliability assessments; in large organized markets transmission operators may not be appropriate for this purpose because they do not have a wide-area view.

864. While we did not address review time frames in the NOPR, we are in general agreement with EEI's suggestion that "near-real time" system review by reliability coordinators may be more practical, while still being efficient and effective in achieving reliability goals. A proactive approach, i.e. one that involves reliability coordinators in a way that permits them to make wide-area assessments of composite interchange transactions for purposes of evaluating reliability impact, including identifying potential IROL violations and mitigating them using TLR procedures before they become actual IROL violations, is far superior to a reactive approach, i.e., one that brings reliability coordinators in after the fact to invoke TLR procedures to avoid an IROL violation or other operating actions to extricate the system from reliability problems such as an actual IROL violation.

865. The Commission stated in Order No. 672 that it expected entities to use the

Reliability Standards development process to address their concerns about a Reliability Standard. With respect to CAISO's request that the Commission consider whether the Western Interconnection needs to comply with these Requirements at all or whether a transition period is appropriate, since CAISO did not raise either concern in the Reliability Standards development process, and others in the Western Interconnection have not raised a similar concern, CAISO should raise this issue in the Reliability Standards development process in the first instance. Reliability Standard INT-006-1 will apply to CAISO.

866. Accordingly, the Commission approves Reliability Standard INT-006-1 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to INT-006-1 through the Reliability Standards development process that: (1) makes it applicable to reliability coordinators and transmission operators and (2) requires reliability coordinators and transmission operators to review energy interchange transactions from the wide-area and local area reliability viewpoints respectively and, where their review indicates a potential detrimental reliability impact, communicate to the sink balancing authorities necessary transaction modifications before implementation.

[288] NOPR at P 219.

We also direct that the ERO consider the suggestions made by EEI and TVA and address the questions raised by Entergy and Northern Indiana in the course of the Reliability Standards development process.

j. Interchange Confirmation (INT-007-1)

867. Reliability Standard INT-007-1 requires that before changing the status of submitted arranged interchanges to confirmed interchanges, the interchange authority must verify that the submitted arranged interchanges are valid and complete with relevant information and approvals from the balancing authorities and transmission service

providers. The Commission proposed in the NOPR to approve INT-007-1 as mandatory
and enforceable.

i. Comments

868. APPA agrees with the Commission that INT-007-1 is sufficient for approval as a
mandatory and enforceable Reliability Standard, subject to NERC's plans for the registration of entities as interchange authorities.

ii. Commission Determination

869. The Commission approves Reliability Standard INT-007-1 as mandatory and enforceable. The Commission has set forth above its analysis and conclusion on interchange authorities. Our understanding is that in the interim source and sink balancing authorities will serve as interchange authorities until the ERO has clarified the
role and responsibility of an interchange authority in the modification of Functional
Model and in the registration process.

k. Interchange Authority Distribution of Information (INT-008-1)

870. INT-008-1 requires the interchange authority to distribute information to all balancing authorities, transmission service providers and purchasing-selling entities
involved in the arranged interchange when the status of the transaction has changed from
arranged interchange to confirmed interchange. The Commission proposed in the NOPR
to approve INT-008-1 as mandatory and enforceable.

i. Comments

871. APPA agrees with the Commission that INT-008-1 is sufficient for approval as a
mandatory and enforceable Reliability Standard, subject to NERC's plans for the registration of entities as interchange authorities. It suggests that NERC should clarify
which reliability entities have the responsibility for ensuring that interchange information
Docket No. RM06-16-000 - 242 -
is coordinated between the source and sink balancing authorities before implementing the
Reliability Standard. APPA also states that NERC should modify this Reliability Standard to make clear what entities it in fact would apply to.

ii. Commission Determination

872. The Commission approves Reliability Standard INT-008-1 as mandatory and enforceable. The Commission has set forth above its analysis and conclusion on

interchange authorities. Our understanding is that a source and sink balancing authority
will serve as the interchange authority until the ERO has clarified the role and responsibility of an interchange authority in the modification of the Functional Model and
in the registration process. Finally, we direct the ERO to consider APPA's suggestions in
the Reliability Standards development process.

l. Implementation of Interchange (INT-009-1)

873. Reliability Standard INT-009-1 seeks to ensure that the implementation of an interchange between source and sink balancing authorities is coordinated by an interchange authority. The Commission proposed in the NOPR to approve INT-009-1 as
mandatory and enforceable.

i. Comments

874. APPA agrees with the Commission that INT-009-1 is sufficient for approval as a
mandatory and enforceable Reliability Standard, subject to NERC's plans for the registration of entities as interchange authorities. It suggests that NERC modify its Functional Model to clarify which reliability entities have the responsibility for ensuring
proper implementation of interchange transactions that have received reliability assessments. APPA also suggests that NERC modify this Reliability Standard to make
clear what entities it in fact would apply to.

ii. Commission Determination

875. The Commission approves Reliability Standard INT-009-1 as mandatory and enforceable. The Commission has set forth above its analysis and conclusion on interchange authorities. Our understanding is that a source and sink balancing authority
will serve as the interchange authority until the ERO has clarified the role and responsibility of an interchange authority in the modification of the Functional Model and
in the registration process. Finally, we direct the ERO to consider APPA's suggestions
concerning this Reliability Standard in the Reliability Standards development process.

m. Interchange Exemptions (INT-010-1)

876. INT-010-1 allows reliability entities to initiate or modify certain types of interchange schedules under abnormal operating conditions and to be exempt from compliance with other INT Reliability Standards.

877. The Commission explained in the NOPR that Reliability Standard INT-010-1

includes provisions that allow modification to an existing interchange schedule or submission of a new interchange schedule that is directed by a reliability coordinator to address current or imminent reliability-related reasons. The Commission interpreted these current or imminent reliability-related reasons as not including actual IROL violations, since they require immediate action so that the system can be returned to a secure operating state as soon as possible and no longer than 30 minutes after a reliability-related system interruption – a period that is much shorter than the time that is expected to be required for new or modified transactions to be implemented.

878. The Commission proposed to approve INT-010-1, interpreted as set forth above, as mandatory and enforceable.

i. Comments

879. Northern Indiana supports the Commission's interpretation of INT-010-1, but it requests that the Reliability Standard be modified to explicitly state that it does not include actual IROL violations.

880. ISO-NE supports Commission approval of INT-010-1, but does not share the Commission's concerns regarding the initiation or modification of interchange schedules to address SOL or IROL violations. It states that interchange schedules can in certain circumstances provide an additional effective tool to help prevent an SOL and IROL violation. While ISO-NE recognizes that other tools may in certain circumstances be more effective, it states that this neither diminishes the value nor precludes the use of the tools contained in INT-010-1. ISO-NE also notes that section 2.4 of INT-010-1, which describes Level 4 Non-Compliance, should be edited to state that "[t]here shall be a level four non-compliance. . . " instead of "[t]here shall be a level three non-compliance. . . ."

881. APPA agrees with the Commission that INT-010-1 is sufficient for approval as a mandatory and enforceable Reliability Standard, but APPA does not agree with the Commission's interpretation of the Reliability Standard. APPA explains that the stated

purpose of INT-010-1 is to allow certain types of interchange schedules to be initiated or modified by reliability entities and to be exempt from compliance with other interchange standards under abnormal operating conditions. This Reliability Standard in effect authorizes reliability coordinators to direct, and balancing authorities to take, remedial

actions to adjust interchange schedules immediately and then document these actions after the fact. INT-010-1 thus provides the emergency waiver from other INT Reliability Standards that makes adjusting interchange schedules the appropriate response to a SOL or IROL. APPA states that the Commission's proposed interpretation therefore should not be adopted.

882. EEI cautions against adopting the Commission's interpretation of INT-010-1. EEI believes that the existing standard meets the Commission's expectation, i.e., permitting and encouraging immediate action to alleviate an SOL or IROL. EEI explains that without INT-010-1, all interchange scheduling and schedule modifications would go through the normal process contained in INT-005 through INT-009. Only INT-010 would allow a balancing authority to make an immediate interchange action without obtaining a Tag. Within 60 minutes of the action, the balancing authority would follow up with the necessary documentation and carry forward the action, if necessary. In the absence of INT-010-1, a balancing authority taking such action would be in violation of INT-009 for failing to comply with the normal process requirements.

883. EEI notes by way of example that, to relieve an SOL or IROL, a reliability coordinator requires immediate offsetting changes in the net scheduled interchange of ACE equations of source and sink balancing authorities. Within 60 minutes following the action, the reliability authority directs the balancing authority to reflect the schedule change event using an arranged interchange. The tagging activity ensures coordination

going forward and provides a written record. All of this takes place after the operational
tasks pertaining to the action to alleviate the SOL or IROL, consistent with Commission
expectations.

ii. Commission Determination

884. For the reasons and interpretation noted in the NOPR, the Commission approves
INT-010-1 as mandatory and enforceable.

885. The Commission believes that our interpretation of INT-010-1 is consistent with
the way APPA and EEI understand the Reliability Standards. The Commission believes
that making a modification to an existing interchange schedule on paper for current or
imminent reliability-related situations involving actual IROL violations is ineffective
because its implementation usually takes much longer than the 30 minutes period that is
allowed in the relevant IRO or TOP Reliability Standards. However, the Commission
interprets INT-010-1 as allowing the actual physical transaction to be modified to
alleviate an IROL event without first documenting the modification. The interchange
schedule would then be modified after the fact to document the physical actions taken.

886. With regard to ISO-NE's statement that interchange schedules can, in certain
circumstances, provide an additional effective tool to help prevent SOL and IROL
violations while other tools may, in certain circumstances, be more effective, the
Commission clarifies that our concern is related to using interchange schedules to address
actual IROL violations. We have no concern in using this as a tool help prevent potential
SOL and IROL violations as asserted by ISO-NE. We further note that the phrase in
Requirements R2 and R3 "current or imminent reliability-related reasons" can be
interpreted as potential or actual IROL violations set forth in the comments from
Northern Indiana, ISO-NE, APPA and EEI, and therefore modifications to INT-010-1 are
needed.

887. Accordingly, the Commission approves Reliability Standard INT-010-1 as
mandatory and enforceable. In addition, we adopt the interpretation set forth in the

NOPR that these current or imminent reliability-related reasons do not include actual IROL violations, since they require immediate control actions so that the system can be returned to a secure operating state as soon as possible and no longer than 30 minutes after a reliability-related system interruption – a period that is much shorter than the time that is expected to be required for new or modified transactions to be implemented.

Finally, we direct the ERO to consider Northern Indiana and ISO-NE's suggestions in the Reliability Standards development process.

2009-03 Interchange Information

Standards Involved:

INT-001 — Interchange Transaction Tagging
INT-003 — Interchange Transaction Implementation
INT-004 — Interchange Transaction Modifications
INT-005 — Interchange Authority Distributes Arranged Interchange
INT-006 — Response to Interchange Authority
INT-007 — Interchange Confirmation
INT-008 — Interchange Authority Distributes Status
INT-009 — Implementation of Interchange
INT-010 — Interchange Coordination Exemptions

Research Needed:

None

Purpose/Industry Need (for SAR):

The purpose of revising these standards is to:
1. Provide an adequate level of reliability for the North American bulk power systems - the
standards are complete and the requirements are set at an appropriate level to ensure reliability.
2. Ensure they are enforceable as mandatory reliability standards with financial penalties - the
applicability to bulk power system owners, operators, and users, and as appropriate particular
classes of facilities, is clearly defined; the purpose, requirements, and measures are resultsfocused
and unambiguous; the consequences of violating the requirements are clear.
3. Incorporate other general improvements described in the standards development work plan.
4. Consider comments received during the initial development of the standards and other comments received from ERO regulatory authorities and stakeholders, as noted in the attached review sheets.
5. Satisfy the standards procedure requirement for five-year review of the standards.

2009-03 Interchange Information

Industry Need (for SAR):

INT-001, INT-003 and INT-004 are Version 0 standards that received only minor modifications when INT-005 through INT-010 were developed. As the electric reliability organization begins enforcing compliance with reliability standards under Section 215 of the Federal Power Act in the United States and applicable statutes and regulations in Canada, the industry needs a set of clear, measurable, and enforceable reliability standards. The Version 0 standards, while a good foundation, were translated from historical operating and planning policies and guides that were appropriate in an era of voluntary compliance. The Version 0 standards and recent updates were put in place as a temporary starting point to stand up the electric reliability organization and begin enforcement of mandatory standards. However, it is important to update the standards in a timely manner, incorporating improvements to make the standards more suitable for enforcement and to capture prior recommendations that were deferred during the Version 0 translation.

Brief Description (for SAR):

Most of these are new standards that were approved in 2006. In 2007 and 2008, the standards staff will collect feedback on the strengths and weaknesses of this set of standards from the Operating and Planning Committees and from compliance personnel. The data collected will be used to determine the scope of this project.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Standard Review Form
Project 2009-03 Interchange Information

Standard # INT-001-1 Comments

Title Interchange
Information
Okay

Purpose What is the reliability analysis service?
Need benefit or value proposition.

Applicability Okay

Requirements *Conditions* Okay
Who? WECC & MISO regional differences noted but not in text.
Shall do what? R1 & 2 – define ensure
Result or Outcome Missing

Measures Addressed by Compliance Elements Standard Drafting Team

To Do List FERC NOPR
o Include Measures and Levels of Non-Compliance; and
o Include a Requirement that interchange information must be submitted for all point-to-point transfers entirely within a balancing authority area, including all grandfathered and "non-Order No. 888" transfers.
FERC staff report
o Measure insufficient and non-compliance lacking
o Expecting new standard in November
V0 Industry Comments
o R1 - Too stringent
o R1 – Who tags dynamic schedules?
o Load PSE responsibility is new restriction
o Clarify tagging of reserves
o R2.2 – 60 minute time frame questioned
o Question on generation scheduling
o Onerous to BA's
o More commercial problem than reliability
o Lack of compliance
VRF comments
o R1, 1.1, 2, 2.1, 2.2 – commercial and administrative

Misc. Items Compliance not specified.

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-003-1 Comments

Title Interchange
Transaction
Implementation
Okay

Purpose Need benefit or value proposition.
Don't need names.

Applicability Okay

Requirements *Conditions* Okay
Who? MISO differences cited but not in text.
Shall do what? Okay
Result or Outcome Okay

Measures Addressed by Compliance Elements Standard Drafting Team.

To Do List FERC NOPR
o Include Measures and Levels of Non-Compliance
FERC staff report
o Lack of Measures and Compliance
o Expecting new standard in November
VRF Comments
o R1, 1.1, 1.1.2, 1.2 – commercial and administrative

Misc. Items Compliance not specified but does appear in Compliance Elements Standard Drafting Team version.

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-004-1 Comments

Title Dynamic
Interchange
Transaction
Modifications
Okay

Purpose Okay

Applicability Need to check applicability for LSE & GOP as per SAR.

Requirements *Conditions* Okay
Who? WECC regional difference cited but not in text.
Shall do what? R1 is about reloading the transaction.
Result or Outcome Missing

Measures Only present for R2.
Need to define evidence.

To Do List FERC NOPR
o Include Measures and Levels of Non-Compliance
FERC staff report
o Should include GO & LSE
o Lack of Measures and Non-Compliance
o Timing considerations
V0 Industry Comments
o Replace TSP with TOP
o Need to address tag curtailment
o Suggested non-compliance levels
o Non-compliance based on %
o Use WECC criteria
VRF comments
o R2, 2.2, 2.3 – commercial and administrative

Misc. Items Non-compliance not specified.

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-005-1 Comments

Title Interchange
Authority Distributes
Arranged
Interchange
Okay

Purpose Okay

Applicability Okay

Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing

Measures Define evidence - should include confirmation of receipt.

To Do List FERC NOPR
o Include Measures and Levels of Non-Compliance
FERC staff report
o Not reviewed
VRF comment
o R5 – administrative

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-006-1 Comments

Title Response to
Interchange
Authority
Okay

Purpose Title & Purpose don't align.

Applicability Okay

Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing

Measures Measure does not address the sub-bullets and evidence must be defined.

To Do List FERC NOPR
o Make it applicable to reliability coordinators and transmission operators; and
o Require reliability coordinators and transmission operators to review composite transactions from the wide-area reliability viewpoint and, where their review indicates a potential detrimental reliability impact communicate to the sink balancing authorities necessary transaction modifications prior to implementation.

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-007-1 Comments

Title Interchange
Confirmation
There is nothing about confirmation in the text.

Purpose Same purpose statement as INT-006-1 – doesn't fit here.

Applicability Okay

Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing

Measures Measure only addresses verification of the data.
Also need to define evidence.

To Do List FERC NOPR
o No changes identified.
VRF comment
o R1, 1.1, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.4 – administrative

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-008-1 Comments

Title Interchange
Authority Distributes
Status
Status of what?

Purpose Purpose is about coordination, not just distribution.
Need benefit or value proposition.

Applicability Missing BA, TSP, PSE & RRO.

Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing

Measures M1 - Need to define evidence - should include wording on receipt of message; 2nd sentence is a requirement.
M1.1 – define evidence.

To Do List FERC NOPR
o No changes identified.
VRF comments
o R1.1.1 & 1.1.2 – commercial and administrative

2009-03 Interchange Information

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-009-1 Comments

Title Implementation of
Interchange
Okay

Purpose Need benefit or value proposition.
Don't need names.

Applicability Okay

Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing

Measures M2 & M3 should be sub-bullets of M1.
Define demonstrate.

To Do List FERC NOPR
o No changes identified.

Standard Review Form

Project 2009-03 Interchange Information

Standard # INT-010-1 Comments

Title Interchange
Coordination
Exemptions
Okay
Purpose Need benefit or value proposition.
Applicability Okay
Requirements *Conditions* Okay
Who? Okay
Shall do what? Okay
Result or Outcome Missing
Measures Define evidence.
To Do List FERC NOPR
o No changes identified.
VRF comments
o R1 & 3 – administrative

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

E-Tag 1.8 Project Implementation Plan

Tentative Dates	Purpose	Location
March 19, 2007	Develop E-Tag 1.8 Project Plan Training Industry Conference Calls • 2 in Eastern Interconnection • 2 in Western Interconnection Interoperability Testing	Conference Call
March 20, 2007	IS Approve E-Tag 1.8 Project Plan (approval may occur during March 19 conference call if a quorum is present)	Conference Call
March 20, 2007	Post for 30-day Industry Comment Period (March 20 – April 20, 2007)	Post on NERC and NAESB websites, Comments to be returned to JISWG list server (details to be worked out)
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)
August 5, 2007	Vendor Development (May 3 – May 5, 2007)	
To Be Determined	Industry Tutorial / Q&A / Information Sharing	Coordinated Webcasts
September 5, 2007	Interoperability Vendor Testing August 5 – September 5, 2007 • NERC / NAESB Facilitation • Set-up Interoperability Examples • Draft site acceptance Test Plan • Etc. (details to be worked out)	
November 2, 2007	Industry Training / User Testing / Workshops (tentatively schedule 4 workshops) / (September 5 – November 2, 2007)	4 Workshops Phoenix (WI) San Diego (WI) Chicago (EI) Atlanta (EI)
December 5, 2007	**E-Tag 1.8 - Implementation**	

Notes:

1) The above dates are tentative and subject to change, depending on obstacles encountered during the implementation of the project plan.
2) This project plan will be approved by the Interchange Subcommittee prior to posting for a 30 day period.
3) Additional meetings, conference calls/webcasts, workshops may be scheduled to support the project plan.

References:	**Officers:**	**Contact Information:**
See NERC IS "Related Files" NAESB JISWG "Calendar" for agendas, minutes and related documents	IS Chair: Alan Boesch IS Vice-Chair: Don Lacen JISWG Co-Chair: Jim Hansen JISWG Co-Chair: Bob Harshbarger	is_plus@nerc.com jiswg@nerc.com vthomason@naesb.org tagven@nerc.com tagging@nerc.com

Electronic Tagging
Functional Specification

Version 1.8.0

PENDING APPROVAL FOR IMPLEMENTATION

March 19, 2007

Joint Interchange Scheduling Work Group

North American Electric Reliability Corporation

Table of Contents

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 Rate 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	
	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	

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, IMPLEMENETED, TERMINATED, CANCELLED.
CONFIRMED	The Composite State of a tag for which the tag creation request is in a state of APPROVED, the ramp start time is prior 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.
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 greater than or equal to the current time, and which has not been cancelled or terminated. This State may transition to TERMINATED.
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.

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.
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 withdrawal for a transaction; location of the actual load.
Sink Balancing Authority (Sink BA)	The Balancing Authority metered area in which load is located
Source	Initial point of injection for a transaction; location for the actual generation facility.
Source Balancing Authority (Source BA)	The Balancing Authority metered area in which generation is located.
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	Software component used to indicate individual approval entity

(Approval)	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 e-Tag, its State, and responds to queries regarding the e-Tags in its possession.[rewrite]
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.
TERMINATED	Composite State that results when the e-Tag Author issues a RequestTagTermination 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	A registered entity that administers the transmission tariff and

Provider (TSP)	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.

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 RequestTagTermination 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). Finally, 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.

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

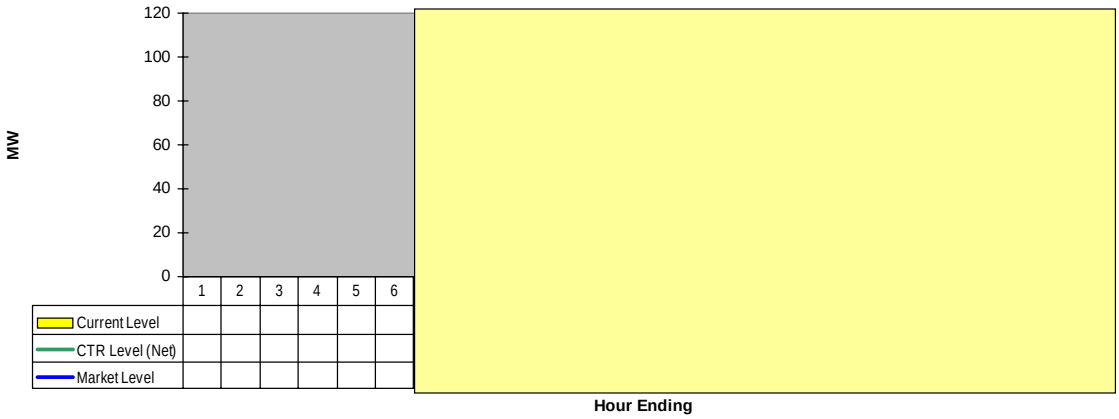
Tag Authors can modify the energy profile up or down without exceeding the Transmission Allocation. Should a curtailment occur for reliability reasons, then the reliability limit must be adjusted to become the new maximum level. The e-Tag Author can modify the energy profile on the e-Tag up or down even 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

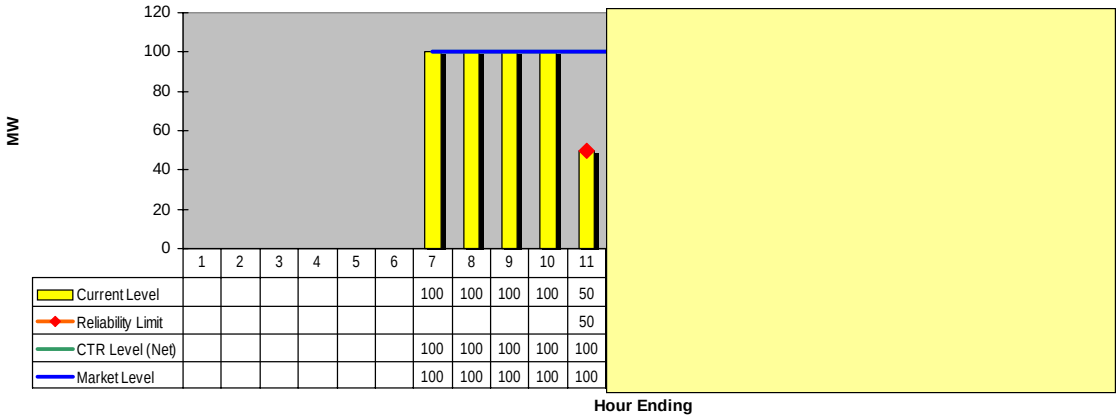
HE7 - HE22 100MW



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

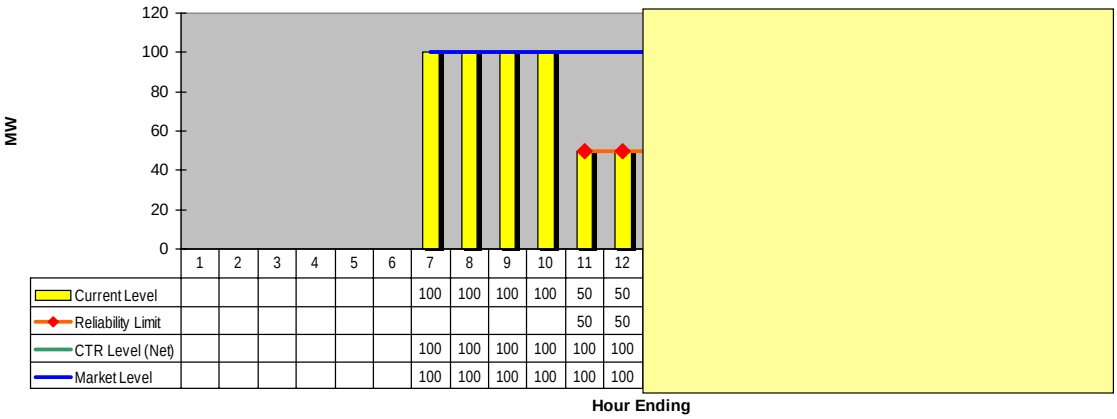
Curtailed to 50MW at 10am



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

STEP 3 – Curtailment Continues

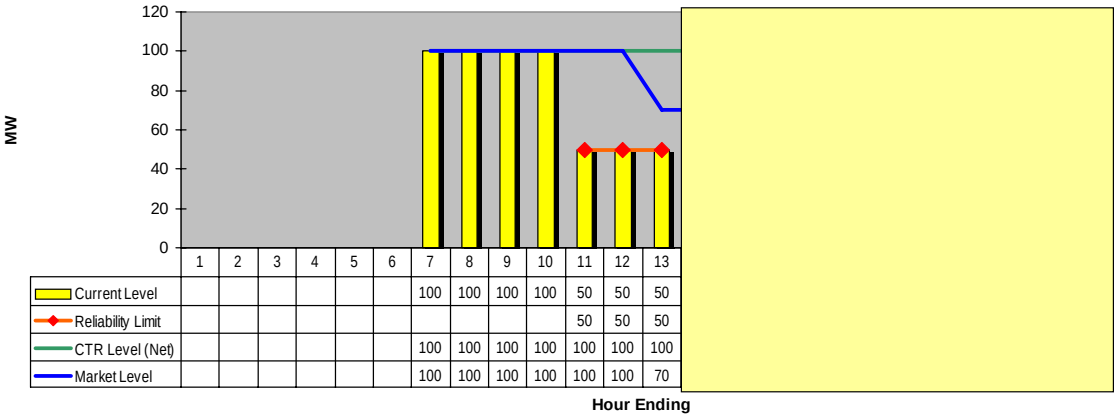
Reissued at each hour



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

STEP 4 – Tag Author Sets Reload Level

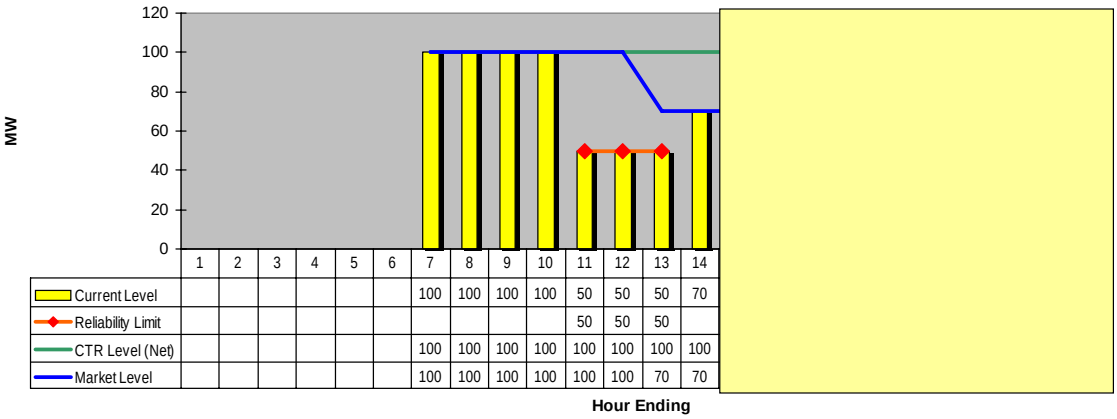
70MW until HE 18



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

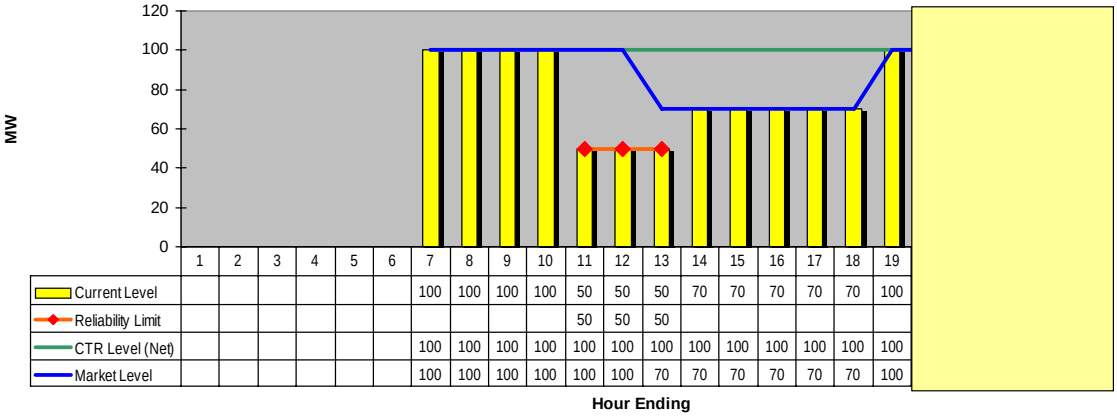


	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Current Level							100	100	100	100	50	50	50	70
Reliability Limit											50	50	50	
CTR Level (Net)							100	100	100	100	100	100	100	100
Market Level							100	100	100	100	100	100	70	70

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

STEP 6 – Tag Fully Reloaded

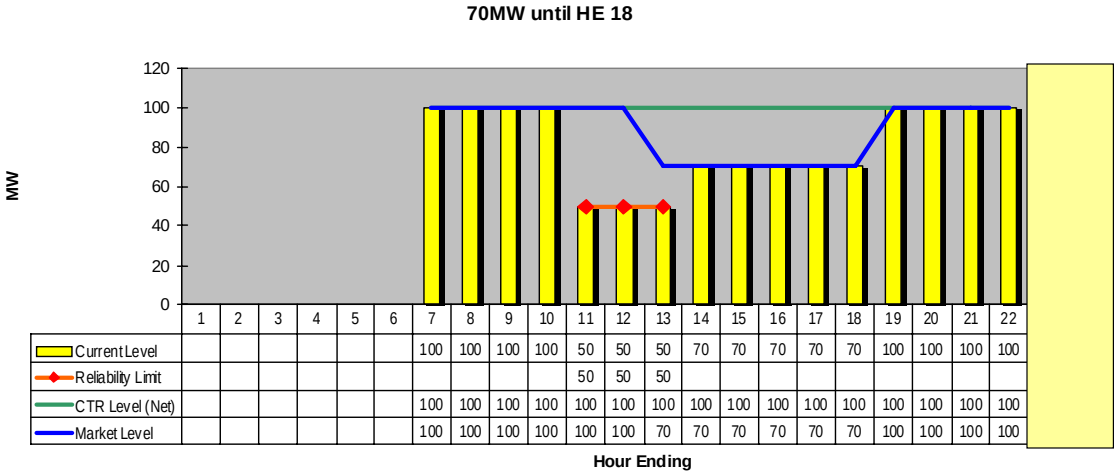
70MW until HE 18



	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



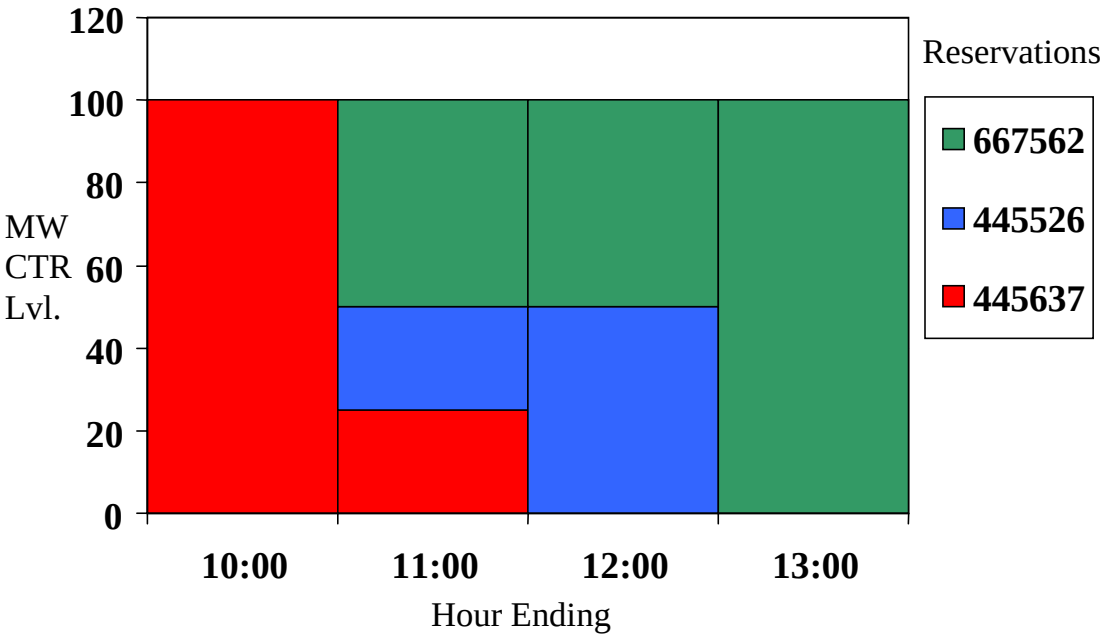
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Current Level							100	100	100	100	50	50	50	70	70	70	70	70	100	100	100	100
Reliability Limit											50	50	50									
CTR Level (Net)							100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
Market Level							100	100	100	100	100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

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.

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 Segment	*Purchasing-Selling Entity*

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 TERIMNATED 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.

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
- DistributeState
- 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 energy profile.

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 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 a TERIMNATED.
- TERMINATED is a final state
- 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. 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 rate for reliability adjustments is zero (this is an instantaneous ramp). 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 zero 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 to the NERC/NAESB Standards timing guidelines. The e-Tag is considered to be LATE or on time as per those guidelines. E-Tags submitted after the e-Tag stop time (as determined by the time of receipt at the Authority and the block end time) 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.

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 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

Once a Correction Request passes validation, the Authority must recomputed 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. 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 1.6.1.3) 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. The description of which entities may change what values is contained in Section 1.6.1.3.
- 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.
- The transmission allocation for all transmission segments must be greater than or equal to the energy profile.

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

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 to supply changes to its 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.

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.

The following diagram illustrates the logical process for distributing a Request. The explanation of the process rules are described immediately following the diagram. Details regarding each specific type of distribution and how its handling varies from the standard process are described in the sections that follow.

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 RequestTagTermination 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.
- RequestTagTermination requests are only allowed for e-Tags that are CONFIRMED, IMPLEMENTED, or TERMINATED.
- The RequestTagTermination 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 RequestTagTermination request is invalid if it requests a start time that is later than or equal to an existing RequestTagTermination Request for the same e-Tag; however, a request for an earlier termination time is allowable.

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:

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

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeTerminateTag
- DistributeProfileChange
- DistributeState
- 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 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 modifying transaction sources or sinks in the Market Operator's market. 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 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.

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 last longer than an hour involving multiple Balancing Authorities. Typically, EMER 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.

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, Source Balancing Authority, or Sink Balancing Authority 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.

6.1.4.2.2.3 Current Level Exceptions

The Current Level will define the level that should be flowing, based on the Base Current Level and the application of all subsequent approved Requests associated with the e-Tag. These requests must be applied in order of receipt by the Authority. This level is intended to supersede current level defined in the Base profile, and should be used to identify proper flow for any given point in time at which an exception exists.

6.1.5 Transmission Allocations

Transmission Allocations are a special kind of profile set that define 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 must be greater than or equal to the energy profile. 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, DistributeState, 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).

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.

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

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

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

Comment Form for 1st Draft of e-Tag 1.8 Specifications

Please use this form to submit comments on the first draft of the E-Tag 1.8 Specifications document and project plan. Comments must be submitted by **April 26, 2007**. You must submit the completed form by email to Tom.Vandervort@nerc.net with the words "E-Tag 1.8 Specifications" in the subject line. If you have questions please contact Tom Vandervort at Tom.Vandervort@nerc.net or at 609-452-8060.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **FRCC** ☐ **MRO** ☐ **NPCC** ☐ **RFC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA – Not Applicable**	☐	1 — Transmission Owners
	☐	2 — RTOs and ISOs
	☐	3 — Load-serving Entities
	☐	4 — Transmission-dependent Utilities
	☐	5 — Electric Generators
	☐	6 — Electricity Brokers, Aggregators, and Marketers
	☐	7 — Large Electricity End Users
	☐	8 — Small Electricity End Users
	☐	9 — Federal, State, Provincial Regulatory or other Government Entities
	☐	10 – Regional Reliability Organizations, and Regional Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact E-mail:

Additional Member Name	Additional Member Organization	Region*	Segment*

*If more than one region or segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on the prior page.

Background Information

The draft E-Tag 1.8 Specifications document was prepared to improve the functionality and ease of use of the E-Tag system. In order to achieve a timely and consistent application of the draft changes, the Joint Interchange Subcommittee Working Group and the NERC Interchange Subcommittee also developed a proposed project plan to implant the changes.

The Joint Interchange Subcommittee Working Group and the NERC Interchange Subcommittee would like to receive industry comments on the proposed revisions to the E-Tag 1.8 specifications.

This latest proposed update to the e-tag specification was driven by changes in both NERC reliability standards and complementary NAESB business practices. The NAESB Executive Committee and the NERC Interchange Subcommittee assigned the e-tag update to the NERC/NAESB Joint Interchange Scheduling Group (JISWG).

The JISWG reviewed both the e-tag schema and specifications and determined that modifications were required for both. Changes to the schema require months of development effort by all e-tag vendors, interoperability testing, and changes to downstream software used by electric industry participants. Modifications were therefore split into two categories: 1) changes that would allow compliance with the Coordinate Interchange Standards effective January 1, 2007 without requiring schema changes, and 2) changes that require schema changes.

Changes in the first category were made to the specification and released as version 1.7.097. This version was implemented January 3, 2007. The transition went smoothly.

Implementation of version 1.8 is expected in late 2007. It should be noted that implementation targets will be driven by successful achievement of milestones such as incorporation of industry comments, interoperability testing, and the amount of time required by industry participants to modify downstream software.

The improvements in e-tag 1.8 include:

1. Full implementation of Coordinate Interchange standards
2. Alignment with the NERC functional model
3. Cleanup of unnecessary sections of the specification
4. Cleanup of unused sections of the schema and specification
5. Addition of missing requirements that have led to implementation variances (such as rounding and ramping)
6. Leveraging of the e-tag infrastructure to allow entities to utilize the e-tag as their primary form of communication
7. Automation of validations required by NERC/NAESB standards
8. Addition of new features requested by industry participants
9. Addition of security based on NAESB PKI standards

What's New or Changed

Below is a summary of what is new or has changed in the E-tag specifications document. The summary is provided as an introduction to the changes and is not intended to replace a review of the E-tag specifications document. Please read it thoroughly.

Specifically, e-tag changes include:

1. Removing Background section
2. Adding reference to default ramp rate definitions

3. Adding new final states and their definitions
4. Adding rounding definition
5. Adding ramp rate validation
6. Identifying physical segment in curtailment (for proper MWh accounting when in-kind losses are used)
7. Modifying in-kind loss calculations
8. Defining which Functional Model entities can be scheduling entities (BA)
9. Removing Appendix A
10. Removing portions of erroneous current level warning
11. Carbon copy list (no approval, sent copies of e-tag)
12. Calculation of ActOnByTime
13. Adding TimeClassification (Late, OnTime, ATF)
14. Revising NERC Web site to Electric Industry Registry Web site
15. Adding TerminateRequest, DistributeTerminate, and DistributeCancel methods.
16. Simplifying the Recovery function
17. Allowing ATF e-tags to be terminated
18. Allowing Source or Sink to modify DYNAMIC e-tag with actual data
19. Specifying that the transmission allocation must be greater than the energy profile
20. Requiring that validations in INT-007-1 R1.1, 1.2, and 1.3 are performed by the agent and authority
21. Adding SSL (secure socket layer) via HTTPS (secure HTTP) and client certificate requirement based on NAESB PKI standard

You do not have to answer all questions.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

1. Do you agree with the new E-tag 1.8 Specifications as modified? If not, please explain your answer.

   ☐ Yes

   ☐ No

   Comments:

2. Do you agree with the timeline suggested in the E-tag project plan? If not, please explain your answer.

   ☐ Yes

   ☐ No

   Comments:

3. The Interchange Subcommittee would like to solicit industry input regarding how the E-Tag system should handle MW hourly/daily rounding. What values should be displayed and how should they be aggregated?

   Comments:

4. Are you aware of any conflicts between the proposed E-tag 1.8 specifications and any regulatory function, rule/order, tariff, rate schedule, legislative requirement or agreement? If yes, please explain your answer.

   ☐ Yes

   ☐ No

   Comments:

5. Do you have other comments on the proposed E-tag 1.8 specifications or project plan? If yes, please describe.

   ☐ Yes

   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 9, 2007

TO: NERC Operating Reliability Subcommittee (ORS)

Dear Members:

Dynamic Schedule Information in the Interchange Distribution Calculator (IDC)

The NERC Standards (INT-004-1 Dynamic Interchange Transaction Modifications) require E-tags for Dynamic Schedules to have an energy profile that reflects a forecast of the average energy expected for the hour. An excerpt from the Standard follows:

R2. The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:
R2.1. The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.
R2.2. The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.
R2.3. A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.

This methodology was specified in the standards to ensure that Dynamic Schedules are adequately reflected in the IDC. The use of average energy forecasts often leads to errors in the IDC and doesn't reflect the worst case from a reliability perspective.

The Interchange Subcommittee (IS) believes that including actual flow data for Dynamic Schedules in the IDC would be a better solution. This information is readily available by participating Balancing Authorities as Dynamic Schedules are required to be metered and included in a Balancing Authorities Area Control Error (ACE) equations. In addition, the practice of using average energy forecasts for Dynamic Schedules is very difficult to monitor for compliance purposes. If metered data can be used in the IDC, then the IS will consider changing the standard to require maximum energy values in the E-tag. This will provide a better reliability solution in forecast hours.

Based on the above, the Interchange Subcommittee requests that the ORS conduct the necessary investigations, utilizing the IDC Working Group if necessary, to determine the feasibility of this approach.

Please feel free to contact the IS if further information is required by either the ORS or IDCWG. We look forward to working with you on this matter.

Yours Truly,

Don Lacen
Vice Chair – Interchange Subcommittee

cc: Interchange Subcommittee
Don Benjamin
Dave Nevius

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

1068. We will require annual caps on the number of hours because calculating an annual cap entails less risk for the transmission provider and its existing firm customers than monthly or seasonal caps. While we will not require monthly or seasonal caps, we encourage transmission providers to offer them if they can overcome modeling barriers because monthly or seasonal caps give more certainty to customers about the particular aspects of their service. Though we allow for flexibility in modeling and determining the number of conditional curtailment hours for a particular service request, we believe that this will have a minimal impact on conditional firm customers. Transmission providers will be allowed to curtail only for reliability purposes and conditional firm customers during conditional curtailment hours will be curtailed only after all point-to-point non-firm customers have been curtailed.

(iii) Conditional Curtailment Priority

Comments

1069. Some commenters agree with the Commission's proposal that conditional firm service should have secondary network curtailment priority during conditional curtailment hours,[656] while others disagree. Bonneville supports the use of the secondary network curtailment priority arguing that customers will value the service more with the secondary network priority, thus increasing the viability of conditional firm service as an alternative to transmission upgrades. EPSA and AWEA argue that conditional firm

[656] E.g., Bonneville, AWEA Reply, and EPSA Reply.

service during conditional curtailment hours should be curtailed after all non-firm uses. In their reply comments, TDU Systems oppose EPSA and AWEA's position, arguing that secondary network service should have at least as high a priority as conditional firm service. In contrast, EEI argues that setting the curtailment priority equal to secondary network service would adversely impact the reliability of firm service by reducing real-time redispatch options and contradict Order No. 888 precedent that provides priority non-firm service only for network customers that pay a load ratio share of system costs.[657] If conditional firm service is implemented, Powerex states that transmission providers should provide data and evidence demonstrating that the rights of existing long-term firm customers will be protected. EEI takes issue with the Commission's proposal to grant conditional firm customers priority non-firm service during conditional curtailment hours because they would pay for long-term use of the grid, stating that all long-term point-to-point customers pay for service on a long-term basis but, unlike network customers, they do not get priority non-firm service.

1070. Commenters address implementation issues related to the Commission's right of first refusal, tagging, tracking, and curtailment priority proposals, as well as other implementation issues implicated in the conditional firm service. Manitoba Hydro, Bonneville and Seattle support the Commission's proposal that conditional firm service would qualify for right of first refusal when firm service becomes available. Several

[657] Citing Order No. 888 at 31,750.

commenters believe that the Commission's proposal with regard to right of first refusal should be refined to allow automatic assignment to conditional firm customers of firm capacity as it becomes available in the short term.[658] Bonneville asserts that prior to implementation of the new service the industry must work with NAESB to develop a communications protocol to either employ automatic assignment or right of first refusal.

1071. Entergy and Exelon state that the standards for implementing transmission loading relief, including the NERC's Interchange Distribution Calculator (IDC), would need modification to allow for curtailment. Specifically, Entergy contends that the Commission should allow time for the IDC to be modified to specify a different curtailment priority for the same transaction depending on the identity of the constraining element. Imperial states that it may take over a year to develop computer software to correctly handle new curtailment priorities during an emergency. Bonneville disagrees and states that conditional firm service does not present unique issues with respect to curtailment and that it would be curtailable during real time like secondary network service.

1072. EEI states that the conditional firm service as currently proposed would conflict with tagging protocols and NERC criteria because there is currently no way to tag service as both firm and non-firm. EEI states that, if conditional firm service is subject to curtailment during a specific period, the tag can identify those periods and curtailments

[658] E.g., EEI, EPSA, TranServ, Bonneville, Constellation and Seattle Reply.

will be implemented in conditional periods and non-conditional periods in accordance with those tags. However, if conditional service is curtailable in a certain number of hours, or when specific conditions occur, the tag cannot be rewritten in a way that will provide for curtailment without personal involvement of balancing authority operators, which could lead to increased curtailments of firm transmission customers.

1073. Xcel states that limiting curtailments to a specified number of hours per year could result in conditional firm service having greater value than firm, while strictly adhering to a maximum number of curtailment hours could potentially conflict with the reliability standards in section 215 of the FPA. NRECA argues that conditional firm service should be subject to pro rata curtailment with all other firm users during non-conditional times.

Commission Determination

1074. We adopt a secondary network curtailment priority to apply for the hours or specific system conditions when conditional firm service is conditional. During non-conditional periods, conditional firm service is subject to pro rata curtailment consistent with curtailment of other long-term firm service. Thus, secondary network service and conditional firm service when it is conditional will share the same curtailment priority. Also, there is no conflict with reliability standards because conditional firm service will be subject to pro rata curtailment with all other firm uses of the system once conditional curtailment hours, if that is the option selected, are exhausted.

1075. The secondary network curtailment priority is appropriate because the customer is paying the long-term firm point-to-point rate and thus should receive the highest non-firm

curtailment priority during the conditional curtailment hours or during specified system conditions. Adoption of this curtailment priority overcomes what could otherwise be significant implementation hurdles. It allows for implementation of the service without changes to existing NERC TLR practices. NERC and members of the industry need not undertake the time-consuming and expensive process of establishing a new curtailment priority that is between firm and non-firm service as some commenters requested. Use of this curtailment priority also avoids attendant decisions relating to the method of curtailment that should apply, i.e., pro rata or transactional curtailment, for a quasi-firm curtailment priority. It is also consistent with existing interruption provisions of the pro forma OATT which provide that secondary service cannot be interrupted for economic reasons.[659] This is consistent with our determination that conditional firm service when it is conditional is curtailable only to maintain reliable operation of the transmission system.

1076. We reject EEI's argument that the curtailment priority for conditional firm service is inconsistent with Commission precedent regarding priority non-firm service only for network customers. EEI's argument is inapposite. Long-term firm point-to-point customers taking fully firm service without the conditional firm option do not need access to priority non-firm service as EEI suggests. They have assurance that their service will not be interrupted for economic reasons and will only be curtailed on a

[659] See pro forma OATT section 14.7.

comparable basis with network service. This would not be the case for conditional firm customers. We also find that EEI has failed to explain the connection between the conditional firm transmission service and the availability of reliability redispatch options, i.e., generators on its system that can ramp up or down in response to a curtailment. We reject Powerex's request that transmission providers be required to show that existing long-term rights are protected. Each addition of a new long-term firm transaction impacts the rights of existing firm customers to some extent.

1077. We disagree with commenters' suggestion that the NERC IDC must be changed to accommodate conditional firm service. We reiterate that we are not creating a new curtailment priority in this Final Rule. We also disagree that new tags that combine a firm and non-firm priority must be developed in order to implement the conditional firm option. The curtailment priority in a tag can be changed ahead of the operating hour based on a near-term forecast of system conditions.[660] We are cognizant that daily and hourly operations to change the tags for conditional firm customers likely involve the need for control room coordination and development of an appropriate tracking process. As the Commission described in the NOPR, new tracking and tagging business practices for this service must be developed by each transmission provider. Thus, we are allowing

[660] For example, in the Eastern Interconnection, tags can be changed up to 35 minutes before the hour in which a TLR event is scheduled. See NERC Standard IRO-006-3, Transmission Loading Relief Procedures – Eastern Interconnection, section 6.2 (Communications and Timing Requirements) at 23-25 (August 2, 2006).

a sufficient period for the development of these business practices, i.e., 180 days from the date of publication of this Final Rule in the Federal Register. As directed above, transmission providers must coordinate with other transmission providers in their regions to develop these tracking and tagging business practices.

1078. Finally, we address requests to allow for automatic assignment of short-term firm point-to-point service to conditional firm customers. We agree that transmission providers must take into account the conditional firm service in evaluating the availability of short-term firm service. Because conditional firm is a long-term firm use of the system, it should not be interrupted prior to short-term firm service. However, short-term firm service reserved prior to the reservation of conditional firm service should maintain priority over conditional firm service in the periods when conditional firm service is conditional, i.e., when specified system conditions exist or conditional curtailment hours apply. Because the assignment proposal meets both of these objectives, we direct transmission providers to assign short-term firm service to conditional firm customers as the service becomes available. Accordingly, we direct transmission providers to work with NAESB to develop the appropriate communications protocols to implement this attribute of conditional firm service. Transmission providers need not implement this requirement until NAESB develops appropriate communications protocols.