NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minutes
Joint Interchange Scheduling Working Group

July 23–24, 2008
Delta Halifax Hotel
Halifax, Nova Scotia

A meeting of the North American Electric Reliability Corporation (NERC) and the North American Energy Standards Board (NAESB) Joint Interchange Scheduling Working Group (JISWG) was held on July 23–24, 2008 in Halifax, Nova Scotia. The meeting announcement, agenda, and attendance list are attached as **Exhibits A**, **B**, and **C**, respectively. JISWG co-chairs Jim Hansen and Bob Harshbarger presided.

Antitrust Compliance Guidelines

Secretary Vandervort acknowledged the NERC Antitrust Compliance Guidelines.

Minutes of the Previous Meetings

The JISWG did not review the May 21–22, 2008 meeting minutes. The JISWG will review the May 21–22, 2008 meeting minutes with these minutes during the September 16, 2008 meeting.

Coordinate Interchange Timing Tables Standard Drafting Team

Co-chair Harshbarger reported that the NERC Coordinate Interchange Timing Tables Standard Drafting Team (CITTSDT) met two times to respond to comments. The CITTSDT considers the comment-related changes made to the Coordinate Interchange Timing Tables to be non-substantive. The latest version of the draft NERC Coordinate Interchange Timing Tables standards, the comments, and the responses will be submitted to the NERC Standards Committee with a recommendation to post the INT-005, INT-006, and INT-008 interchange standards' timing tables for a 30-day pre-ballot posting, followed by a standards ballot.

The announcement, standards revisions, implementation plan, and comment form can be found on the NERC Standards Coordinate Interchange – Timing Table (Project 2007-14) Web site, as follows:

http://www.nerc.com/filez/standards/INT_Urgent_Action.html

e-Tag 1.8.1 Specifications - Comments and JISWG Responses

The JISWG addressed numerous comments received since the May 2008 JISWG meeting and posted the latest "official draft" of the e-Tag 1.8.1 specifications on both the NERC and NAESB Web sites. The draft is not ready for comment but will inform the industry of the progress the JISWG is making to revise the specifications. The official draft e-Tag 1.8.1 specifications are attached as **Exhibit D**.

Proposed Transfer of e-Tag Specifications from NERC to NAESB

The JISWG discussed the informal proposal to transfer the e-Tag specifications and e-Tag schema from NERC to NAESB. The e-Tag specifications have been identified as a gray area within the NERC Reliability Standards process. The e-Tag specifications are not a reliability standard, but are significantly more than just a supporting/reference document. Since NAESB already owns and maintains several technical standards such as OASIS Standards & Communications Protocol and gas pipeline electronic data interchange, it is proper to consider having NAESB become the official sponsor of the e-Tag specifications and e-Tag schema. NAESB already incorporates vendor representation, which seems to support NAESB ownership of the e-Tag specifications.

The transition from NERC to NAESB would give more weight to the e-Tag specifications as a NAESB Business Practice Standard and would ensure that the specifications, schema, and the e-Tag process implementation are reviewed through a process geared toward business practices and software standards. The concept envisions the JISWG developing the NAESB business practice standard. It is also anticipated that NERC and NAESB would remain as the significant participants in electronic tagging specifications development through the JISWG.

Since the electric industry registry (EIR) is transferring from NERC to NAESB, the JISWG believes it also makes sense to transfer the e-Tag specifications and schema from NERC to NAESB.

The JISWG developed the following action Items to begin the transfer of the e-Tag specifications and schema from NERC to NAESB:

1. Paul Sorenson, co-chair, NAESB Electronic Scheduling Subcommittee/Information Technology Subcommittee (ESS/ITS), will discuss the transfer of the e-Tag specifications and schema from NERC to NAESB with the ESS/ITS.
2. Cory Galik, NAESB staff, will investigate if the e-Tag specifications can be a NAESB document other than a NAESB Business Practice Standard.
3. Tom Vandervort, NERC JISWG secretary, will visit with Lynn Constantini at NERC and Rae McQuade at NAESB on the formal process to transfer the e-Tag specifications and schema from NERC to NAESB.
4. The JISWG will develop a NAESB Business Practice Standard request pending the results of ESS/ITS discussion, conclusions, and recommendations on the e-Tag specifications and schema transfer from NERC to NAESB (number 1, above).

The JISWG may have conference calls to discuss the results of the action items above, prior to the next scheduled meeting in September 2008.

WECC Coordinate Interchange Business Practices (WEQ-004)

The NAESB Wholesale Electric Quadrant (WEQ) co-chairs of the Joint Electronic Scheduling Subcommittee/Information Technology Subcommittee (ESS/ITS) and Business Practice Subcommittee (BPS) requested assistance from the JISWG regarding FERC Order 890.

Background

The co-chairs of the Joint ESS/ITS and BPS need the JISWG assistance in completing its Annual Plan Item 2.b.iii.2, "Business practice standards that include an OASIS mechanism to "allow for auditing of "capacity benefit margin" (CBM) usage." The joint subcommittee identified that the audit mechanism could be done through the OASIS scheduledetail. In order to meet this FERC Order 890 requirement something needs to be included in the tag in the e-Tagging system to identify the tag as being capacity benefit margin. The Annual Plan Item 2.b.iii.2 states:

Conclusions

The Joint BPS-ESS/ITS work scope will include:

- Requesting (of JISWG) that something be added to the e-Tag specifications to identify usage of CBM (should verify that the NERC team hasn't already taken care of this and perhaps jointly make the request to JISWG)
- Ensure that the identifier added by JISWG is included in the query parameters scheduledetail template
- Ensure that any changes to the e-Tag spec will not impact other NAESB Business Practice Standards

The ESS/ITS and BPS co-chairs thought the NERC ATCDT may need this information on the tag as well to meet "MOD-004 R.12.1." Needless to say, we are not sure what path we need to follow to request/get changes made to tags so they can be identified as CBM. The ESS/ITS and BPS co-chairs are sure that the Joint ESS/ITS and BPS cannot finalize the Order 890 CBM recommendation until a decision is received from JISWG on how a tag can be identified as CBM. If the decision is to add a new field, we'll have to make a change to the scheduledetail template. If the decision is to add a code value to an existing field, we will need to add that information.

JISWG Discussion and Action

The JISWG discussed the ESS/ITS and BPS request and formalized its recommendation to enhance the NAESB Business Practice Standard WEQ-004 to address the CBM request. The proposed JISWG enhancements to WEQ-004 are attached as **Exhibit E**.

Dates and Locations of Future Meetings

The JISWG May 2009 meeting was changed from a NERC coordinated meeting to a NAESB coordinated meeting. Look for additional information and meeting details on the NERC JISWG Web site and on the NAESB JISWG Web site.

Additional meetings or conference calls may be scheduled as necessary for the implementation of the e-Tag, version 1.8.1 or other JISWG-related business.

JISWG Meeting/Conf Call/Webcast Schedule

	Date	Time	Location	Meeting Coordinator
Meeting	Tues, Sep 16, 2008	8 am – 4 pm	Vancouver, BC	NERC Precedes the IS Meeting
Meeting	Wed, Nov 12, 2008 Thur, Nov 13, 2008	10 am – 5 pm 9 am – Noon	Houston	NAESB
Meeting	Wed, Jan 14, 2009 Thur, Jan 15, 2009	10 am – 5 pm 9 am – Noon	Phoenix	NERC
Meeting	Wed, Mar 11, 2009 Thur, Mar 12, 2009	10 am – 5 pm 9 am – Noon	Houston (or volunteer city)	NAESB
Meeting	Wed, May 13, 2009 Thur, May 14, 2009	10 am – 5 pm 9 am – Noon	Houston (or volunteer city)	NAESB
Meeting	Wed, Jul 15, 2009 Thur, Jul 16, 2009	10 am – 5 pm 9 am – Noon	Toronto	NERC
Meeting	Wed, Sep 16, 2009 Thur, Sep 17, 2009	10 am – 5 pm 9 am – Noon	Houston (maybe Seattle)	NAESB
Meeting	Wed, Nov 18, 2009 Thur, Nov 19, 2009	10 am – 5 pm 9 am – Noon	Houston (or volunteer city)	NAESB

Respectfully submitted,

Tom Vandervort

Thomas J. Vandervort
NERC JISWG Secretary

Angie Nicastro

From: Angie Nicastro [Angie.Nicastro@nerc.net]
Sent: Friday, June 13, 2008 9:57 AM
To: Angie Nicastro
Subject: MEETING: July 2008 Joint Interchange Scheduling Working Group
Attachments: NERC JISWG.vcs; footer

Exhibit A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Announcement:
Joint Interchange Scheduling Working Group
July 23-24, 2008 | Halifax, Nova Scotia

Register online today: http://www.nerc.net/meetingregistrations/Committee.aspx?meetingdate=7/23/2008&meetingtype=JISWG

Meeting Group and Dates	
Group Name	Joint Interchange Scheduling Working Group
Dates	7/23/2008 -- 1:00 PM - 5:00 PM 7/24/2008 -- 10:00 AM - 5:00 PM
Hotel	
Hotel	Delta Halifax
Address	1990 Barrington St
City	Halifax
State	NS B3J1P2
Phone	902-425-6700
Fax	
Cut-Off Date	7/2/2008
Attending Staff	
Staff	Tom Vandervort
Miscellaneous	
Notes	**PLEASE CALL THE HOTEL DIRECTLY TO BOOK RESERVATIONS** Hotel Location- map • Room Block Code: NERC • Room rate: $149 single/double occupancy • Room block: Nights of July 23, 2008 - There are a limited amount of rooms are available. • Check-in: 3 p.m., Check-out: noon • Check with the hotel directly for early cancellation/departure fees. • Hotel cut-off date: July 2, 2008. NOTE: After the cut-off date the hotel will release this block of rooms and only accept reservations on a space-available basis at the prevailing room rate. • Dress code: Business casual

When making your hotel reservation, please be sure to mention the "NERC" to get the preferred rate and ensure your reservation is credited to the NERC room block. The hotel will charge NERC a penalty if the total rooms blocked for this event are not picked up. Also, if you use a travel agency for your travel plans, please make sure the agency mentions NERC. For more information or assistance, please contact Angie Nicastro, Administrative Assistant, at angie.nicastro@nerc.net or at (609) 452-8060.

Attached please find an outlook meeting invitation. If you would like to add it to your schedule, just double click on the attachment, select "Open" from the pop up screen, and then hit the "Save & Close" button at the upper left hand of the meeting screen to add to your calendar.

Angie Nicastro
Administrative Assistant
North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Exhibit B

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

Joint Interchange Scheduling Working Group Meeting

Wednesday, July 23, 2008 — 1–5 p.m. Atlantic Daylight Time
Thursday, July 24, 2008 — 10 a.m.–5 p.m. Atlantic Daylight Time
Delta Halifax Hotel
1990 Barrington St.
Halifax, NS B3J1P2
Hotel Phone: (902) 425-6700

Conference Bridge (Call-in):
Wednesday Phone Number: (732) 694-2061
Wednesday Access Code: 1123072308#
Thursday Access Code: 1123072408#

Participation via WebEx Webcast
Location: https://nerc.webex.com/nerc
Topic: JISWG
Wednesday Password: 072308
Thursday Password: 072408

Agenda

1. **Administrative**
   a. Membership and Guests — Chair
   b. Arrangements — Secretary
   c. Approval of Meeting Minutes
      i) May 21–22, 2008 Meeting Minutes — Chair
   d. Procedures
      i) Parliamentary Procedures — Secretary
      ii) Antitrust Compliance Guidelines — Secretary
   e. Approval of Agenda — Chair

2. **Coordinate Interchange Timing Tables Standard Drafting Team —** Chair

3. **NAESB Confidentiality Agreement —** Chair

4. **NAESB Electric Industry Registry (EIR) Transition from NERC to NAESB —** Chair

5. **EIR Cleanup —** Chair

6. **e-Tag Specifications Version 1.8.1 Development —** Chair

7. **Informal Proposal to Transfer e-Tag Specifications from NERC to NAESB —** Chair

8. **Capacity Benefits Margin —** Chair

9. **Future JISWG Meetings/Conference Calls —** Chair
   a. Review Meeting Dates, Start and End Times
   b. NERC-hosted Meeting Guidelines
   c. Future JISWG Meetings Conference Calls/Webcast Schedule

September 16, 2008	Vancouver
November 12–13, 2008	Houston
January 14–15, 2009	Phoenix
March 11–12, 2009	Houston
May 13–14, 2009	Monterey, CA
July 15–16, 2009	Toronto
September 16–17, 2009	Houston
November 18–19, 2009	Houston

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

Joint Interchange Scheduling Working Group Meeting

Wednesday, July 23, 2008 — 1 p.m.–5 p.m. ADT
Thursday, July 24, 2008 — 10 a.m.–5 p.m. ADT
Delta Halifax Hotel
1990 Barrington St.
Halifax, NS B3J1P2

ATTENDANCE

Attended Meeting
Bob Harshbarger (Co-chair - OATI)
Jim Hansen (Co-chair – NERC)
Mark Sundsten (Sungard Energy Systems)
Tom Vandervort (NERC)

Via Phone
Jim Cyrulewski
Pat Terris
Ernie Cardone
Cory Galik
Phillip Shafeei
Tim Kannel
Paul Sorenson
Clint Aymond
Don Lacen
Kristy Humphrey
Mark Nielson
Nik Browning
Robert Sullivan
Troy Simpson

Exhibit D

Electronic Tagging
Functional Specification

Deleted: 0

Version 1.8.1

NOT YET APPROVED FOR IMPLEMENTATION

November 7, 2007

Joint Interchange Scheduling Work Group

North American Electric Reliability Corporation

Table of Contents

Deleted: 4
Deleted: 10
Deleted: 4
Deleted: 10
Deleted: 4
Deleted: 10
Deleted: 4
Deleted: 10
Deleted: 4
Deleted: 10
Deleted: 4
Deleted: 12
Deleted: 4
Deleted: 20
Deleted: 4
Deleted: 23
Deleted: 4
Deleted: 24
Deleted: 4
Deleted: 25
Deleted: 4
Deleted: 27
Deleted: 4
Deleted: 27
Deleted: 4
Deleted: 28
Deleted: 4
Deleted: 29
Deleted: 4
Deleted: 33
Deleted: 4
Deleted: 34
Deleted: 4
Deleted: 35
Deleted: 4
Deleted: 36
Deleted: 4
Deleted: 36
Deleted: 4
Deleted: 37
Deleted: 4
Deleted: 37
Deleted: 4
Deleted: 37
Deleted: 4
Deleted: 38
Deleted: 4
Deleted: 38
Deleted: 4
Deleted: 39
Deleted: 4
Deleted: 40

Deleted: 4
Deleted: 58
Deleted: 4
Deleted: 58
Deleted: 4
Deleted: 59
Deleted: 4
Deleted: 59
Deleted: 4
Deleted: 59
Deleted: 4
Deleted: 59
Deleted: 4
Deleted: 60
Deleted: 4
Deleted: 61
Deleted: 4
Deleted: 61
Deleted: 4
Deleted: 68
Deleted: 4
Deleted: 70
Deleted: 4
Deleted: 72
Deleted: 4
Deleted: 74
Deleted: 4
Deleted: 78
Deleted: 4
Deleted: 77
Deleted: 4
Deleted: 78
Deleted: 4
Deleted: 78
Deleted: 4
Deleted: 79
Deleted: 4
Deleted: 79
Deleted: 4
Deleted: 79
Deleted: 4
Deleted: 79
Deleted: 4
Deleted: 80
Deleted: 4
Deleted: 82
Deleted: 4
Deleted: 83
Deleted: 4
Deleted: 85
Deleted: 4
Deleted: 85

Deleted: 4
Deleted: 101
Deleted: 4
Deleted: 101
Deleted: 4
Deleted: 101
Deleted: 4
Deleted: 103
Deleted: 4
Deleted: 104
Deleted: 4
Deleted: 105
Deleted: 4
Deleted: 106
Deleted: 4
Deleted: 106
Deleted: 4
Deleted: 106
Deleted: 4
Deleted: 107
Deleted: 4
Deleted: 108
Deleted: 4
Deleted: 109
Deleted: 4
Deleted: 110
Deleted: 4
Deleted: 112
Deleted: 4
Deleted: 114
Deleted: 4
Deleted: 115

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

Deleted: ¶

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

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

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

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

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

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

1.1.3 Change Log

Version	Change	spare
1.7096	Accepted all changes in 1.7095 posted document	
	Replaced NERC policy references with NERC/NAESB Standards references	
	Incorporated Functional Model language	
	Added Change Log	
	Updated other references and URLs	
	Market Re-dispatch (MRD) language and function removed	
1.7.097	Removed Passive Approval by Reliability Entities	
	Extend e-Tag creation to 48 hours into the past	
	Extend e-Tag adjustment to 96 hours into the past for DYNAMIC e-Tags	
	Remove 24 hour limit on Reliability Adjustments	
	Remove Counter Party Reports	
	Remove references to MRD	
	Add Optional Approval Rights for any PSE cited in the transmission allocation	
	Replaced various state diagrams with descriptive wording	
	Strike automatic approval of cancellations	
1.8	Remove Background section	
	Add reference to default ramp rate definitions	
	Add new final states and their definitions	
	Add Rounding definition	
	Add Ramp Duration validation	
	Identify physical segment in Curtailment (for proper MWh accounting when in-kind losses are used)	
	Modify in-kind loss calculations	
	Define which Functional Model entities can be Scheduling Entities (BA)	
	Strike Appendix A	
	Strike erroneous current level warning	
	Carbon Copy list (no approval, sent copies of e-Tag)	
	Calculation of ActOnByTime and ImplementTime	
	Addition of TimeClassification (Late, OnTime, ATF)	
	NERC web site changed to Electric Industry Registry web site	
	Added RequestTerminateTag and related handling	
	Simplify Recovery function	
	Allow ATF e-Tags to be Terminated	
	Allow Source or Sink to modify DYNAMIC e-Tag with actual data	

Formatted Table
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered
Formatted: Centered

	Transmission Allocation must be ≥ energy profile.		Formatted: Centered
	Validations in INT-007-1 R1.1, 1.2, and 1.3 are performed by the Agent and Authority		Formatted: Centered
	Added SSL via HTTPS and client certificate requirement based on NAESB PKI standard		Formatted: Centered
	Extend e-Tag creation to 168 hours into the past		Formatted: Centered
	Extend e-Tag adjustment to 168 hours into the past for DYNAMIC e-Tags		Formatted: Centered
	Current Level no longer distributed (calculated based on approved requests in request order)		Formatted: Centered
	Change Tag Agent, Tag Approval, Tag Authority to Agent, Approval, Authority		Formatted: Centered
	Change Tag to e-Tag		Formatted: Centered
	Add Pseudo Tie tag type.		Formatted: Centered
	Add functionality to allow TSP to modify their associated physical segment's Transmission Product Reference and Transmission Allocation(s) with no approval process for support of Order 890 Conditional Firm		Formatted: Centered
	Transmission and Energy profiles must have same earliest start and latest end. Loss Accounting Profile must be bounded by (be within) these.		Formatted: Centered
1.8.1	Modified CANCELLED definition		Formatted: Centered
	Added statement regarding specification/schema relationship		Formatted: Centered
	Modified sections 1.4.1.2 and 3.6.1.1.1 regarding forwarding URLs and the creation of the distribution list		Formatted: Centered
	Modified section 1.4.9.4 to clarify the Authority Service archive requirements		Formatted: Centered
	Made multiple changes to support a 25 hour day		Formatted: Centered
	Added language addressing profile start times and durations in section 2.6.1.1, 3.6.1.1,		Formatted: Centered
	Clarified that entities may not be added or removed in profile change requests in section 2.6.1.3, 3.6.1.3, and 4.6.1.2 and deleted text in 3.6.2.3		Formatted: Centered
	Removed the requirement to include a reason when withdrawing a request in section 2.6.3.2, 3.6.3.2, and 4.6.3.2		Formatted: Centered
	Minor wording correction in 3.4		Formatted: Centered
	Removed a validation item in section 3.6.3.1		Formatted: Centered
	Corrected the spelling of Authority operator in several places		Formatted: Centered
	Added requirement for Authority service to set ActOnByTime and TimeClassfifcation in section 3.6.3.2 and in 3.6.3.3		Formatted: Centered
	Added requirement for asynchronous response in section 3.6.5.2		Formatted: Centered
	Deleted bullet item from section 4.6.3.1		Formatted: Centered
	Revised references to PKI in section 7.1.1		Formatted: Centered

	Still to do – add roll-out document text	
	Still to do – attach regional special appendix	
	Still to do – provide modifications for multiple reliability limits	

Formatted: Centered

Formatted: Centered

Formatted: Centered

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	The collection of generation, transmission, and loads within the

(BAA)	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 Composite State of the e-Tag changes from CONFIRMED to CANCELLED as soon as the Request becomes APPROVED. The Authority sets the market level and transmission allocation of the e-Tag to zero. Once reached, this state may not transition to any other state.
COMMFAIL	A Delivery State indicating that communications were unable to be established between the sender of a message and the recipient.
Composite State	This is the overall state of the e-Tag which can have any of the following values: CONFIRMED, IMPLEMENTED, CANCELLED, PENDING, WITHDRAWN, TERMINATED, EXPIRED and DENIED.
CONFIRMED	The Composite State of a tag for which the tag creation request is in a state of APPROVED, the ramp start time is greater than or equal to the current time, and which has not been CANCELLED or TERMINATED. This State may transition to IMPLEMENTED, CANCELLED, or TERMINATED.
Correction	A change to a Request e-Tag's composition prior to the expiration of the approval window, as defined in NERC/NAESB standards.
Current Level	The current level is derived based upon all approved e-Tag Requests applied in RequestID order. The current level represents the intended energy transfer at specific points in time. The initial current level is set to the market level for each base profile. The current level will vary by physical segment under certain circumstances ("in-kind" losses for example). The current level may be modified by either approved market level changes or reliability limit changes. The current level is set to the lower of the Exception Reliability Limit or the Effective Market Level which is defined as the current Exception Market Level if one exists or, if none exists, then the Base Market Level.
DC Tie Operator	An entity that operates a DC transmission facility; specifically, one that provides a connection between two different interconnections.

Deleted:

DELIVERED	Delivery State indicating that a particular Request was distributed to and received by a party.
Delivery State	A value used to provide information about a party's receipt of a particular Request.
DENIED	Approval State indicating that a party is unwilling to implement a particular Request. If one or more Approval Entities set their Approval State to DENIED then the resulting Request State will become DENIED upon the expiration of the Request's approval window. Once a Request achieves this state, it cannot transition to any other state.
Electric Industry Registry	Data set provided by the Electric Industry Registry vendor describing entity information, such as name, acronym, phone numbers, service URLs, etc… of registered participants.
e-Tag	Document describing a physical interchange transaction and its associated participants. An e-Tag is the result of one or more requests.
Exception Profile	A profile containing time specific changes to original profile values
Exchange	Amount of energy exchanged between two parties; encompasses both physical interchange and title transfers.
EXPIRED	Approval State and Request State that results when one or more reliability Approval Services fail to actively respond to the IA's assessment distribution before the assessment period ends. Once a Request transitions to this state, it cannot transition to any other state.
Financial Path	Path defining the financially responsible parties of a transaction, detailing ownership of energy across physical movement of energy as well as purely financial.
Generation Providing Entity (GPE)	Merchant selling energy from owned, affiliated, or contractually bound generation.
Implement	Allow energy to be scheduled as described.
IMPLEMENTED	The Composite State of a tag for which the tag creation request is in a state of APPROVED, the ramp start time is less than the current time, and which has not been cancelled or terminated. This State may transition to TERMINATED.
In-Kind Losses	Transmission losses delivered coincident with energy delivery.
Individual Approval State	The Approval State associated with a specific party to the e-Tag.
Individual Delivery States	The Delivery State associated with a specific party to the e-Tag.
Interchange Distribution Calculator (IDC)	NERC tool used to determine curtailments during TLR.

Interchange Transaction	A business exchange between two parties that result in the physical flow of energy from one point to another; a strict definition would indicate that exchange must be from one Balancing Authority to another, but for the purposes of this document, **any** such flow utilizing Point-to-Point service shall be considered an Interchange Transaction.
INVALID	Delivery state indicating that a party received a request distribution, but felt it was not syntactically or semantically correct
Load Serving Entity (LSE)	Marketer purchasing energy with the intent to deliver to and serve an affiliated or contractually bound load.
Market Entity	PSE, GPE, or LSE
Market Level	Desired energy profile for the transaction; level of market-desired flow.
Maximum Reservation Capacity	The commitment of transmission resources to support a particular transaction; typically the same as actual flow.
Minute Boundary	Date/Time value "seconds" are zero.
NA	Special Approval State or Approval State Type indicating that the entity does not have approval rights over the Request or that the Request has not yet been delivered to the entity.
OVERRIDE	Approval State Type indicating the Approval State for the entity was manually overridden by the entity providing the Authority Service.
PASSIVE	Approval State type indicating that the entity was unable to state their intentions within the assessment period and the system has made an automated decision on their behalf.
Passive Approval	An approval that occurred through the expiration of a Request's evaluation window without an active approval; set automatically by the Authority when the expiration occurs. Passive approval is only applicable to non-reliability entities such as GPE, LSE, and PSE (whose transmission rights are cited).
Passive Denial	A denial that occurred through the expiration of a Request's evaluation window without an active approval or denial; set automatically by the Authority when the expiration occurs. Passive denial is only applicable to reliability entities such as BA, SE, and TSP.
PENDING	Initial Request State and Approval State.
Physical Path	The source to sink route (via intermediate transmission paths) between generation and load.
Profile	A time/level matrix that defines an energy flow or other related

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

(Sink BA)	
Source	Initial point of supply for a transaction.
Source Balancing Authority (Source BA)	The Balancing Authority metered area in which generation is located.
State	Either the Request State, Composite State, Individual Delivery State, or Individual Approval State.
Straddle Ramp	Ramp that divides the start ramp duration equally across the profile block start or end time.
STUDY	The approver has actively decided to defer their decision to approve or deny until a later time within their approval window, but wishes to communicate their acknowledgement of the request back to the sender.
Synchronous	Message type in which the requesting message is responded to within the same connection.
Tag	e-Tag
Tag Agent Service (Agent)	Software component used to generate and submit new e-Tags, Corrections, and Profile Changes to an Authority and to receive State information for these requests.
Tag Approval Service (Approval)	Software component used to indicate individual approval entity responses when requested by Authority Service, as well as submit Profile Changes.
Tag Author	Entity that creates and submits an e-Tag; the caller of the Request NewTag method.
Tag Authority Service (Authority)	Software component that receives Agent and Approval Requests and Responses and forwards them to the appropriate Approval Services. Also maintains master copy of an e-Tag (all associated Requests), the Composite State of the e-Tag, etc. and responds to queries regarding the e-Tags in its possession
Tag Code	7 Character code used as part of the e-Tag ID to identify a transaction.
Tag ID	Identifier of the e-Tag represented by combining Source BA code, PSE code, an e-Tag Code, and Sink BA code.
Tag Start Time	The earliest time listed in any part of a tag, including energy, transmission, and loss accounting.
Tag Stop Time	The latest time listed in any part of a tag, including energy, transmission, and loss accounting.
TERMINATED	Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of IMPLEMENTED. The Composite State of the e-Tag

	changes from IMPLEMENTED to TERMINATED once the current time is less than or equal to the termination time. The termination time plus stop ramp duration must be greater than or equal to the current time except in the case of ATF e-Tags which may be terminated up to 168 hours into the past. 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).
Termination Time	The time at which the IMPLEMENTED e-Tag will be transition to TERMINATED. The earliest termination time of approved termination requests associated with the e-Tag is the termination time for the e-Tag.
Test e-Tag	An e-Tag used for diagnostic purposes; does not represent actual transacted business.
Title Transfer	An exchange of energy ownership; may or may not be associated with a physical movement of energy.
Transaction Information System (TIS)	Transaction Information System – currently implemented as e-Tagging.
Transmission Allocation	Set by the e-Tag Author, it is a description of how a reservation or contract is being used in a particular e-Tag. The Transmission Allocation allows the author to specify the duration and megawatt level of the capacity used from a transmission reservation to support the e-Tag transaction.
Transmission Customer (TC)	A PSE specified as owner (rights holder) in a Transmission Allocation in the e-Tag. The PSE may or may not be the energy title holder.
Transmission Service Provider (TSP)	A registered entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
Universal Coordinated Time (UTC)	Time standard used by the e-Tagging System for communication purposes; also referred to as Greenwich Mean Time (GMT).
Valid	Passed syntax checks by an e-Tag Service (i.e. not invalid)
Viewing Rights	The rights of an entity to view transaction details.
WITHDRAWN	Final Request State that results when a request submitter (Tag Author or Adjustment requester) submits a WithdrawRequest message before the Request has reached any other final state (e.g., APPROVED, DENIED, etc.). This state may not transition to any other state.

Formatted: Space Before: 0 pt, After: 0 pt

Deleted: ¶

Formatted: Space Before: 0 pt, After: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Deleted: ¶

Deleted: ¶

1.3 Tagging Terminology

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

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

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

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

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

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

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

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

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

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

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

PENDING - initial Request State

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

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

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

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

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

QUEUED – the Request is scheduled for delivery.

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

COMMFAIL – the Request was undeliverable due to communication problems.

DELIVERED – the Request was successfully delivered.

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

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

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

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

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

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

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

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

Active – an Approval Entity actively selected The Approval State.

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

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

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

Deleted: ¶

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.

Deleted: ¶

CANCELLED – Final Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of CONFIRMED with the termination time in the Request set to the block start time

of the e-Tag. The Authority sets the market level and transmission allocation of the e-Tag to zero. Once reached, this state may not transition to any other state.

TERMINATED – Composite State that results when the e-Tag Author issues a RequestTerminateTag message for an e-Tag with a composite status of IMPLEMENTED with the termination time set after the block start time of the e-Tag. The Composite State of the e-Tag changes from IMPLEMENTED to TERMINATED once the current time is less than or equal to the termination time. 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.

Deleted: ¶
Formatted: Bullets and Numbering

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.

Deleted: ¶

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.**

This specification is accompanied by an XML schema. The schema is intended to reflect the specification. Should the specification and schema conflict the specification is the ruling document.

Formatted: Font: 12 pt

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 registering an URL of an Authority Service. The Authority Service forwards all valid received e-Tag Requests to each entity identified in the transaction as having "approval" or "viewing" rights over that Request (see section 3 for distribution list determination), 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 each entity in the distribution list. 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.

Deleted: providing this service directly or by arranging with a third party to provide this service as its agent.

Deleted: the Approval Service associated with

Deleted: the originating Agent and all Agent and Approval Services associated

Deleted: with the transaction, and to the sink BA's designated forwarding location (e.g., RAS or BA's Reliability Coordinator)

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

1.4.1.3 Approval Service

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

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

1.4.1.4 Reliability Authority Service

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

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

1.4.2 Tag Identification

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

1.4.2.1 E-Tag IDs

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

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

Formatted: Indent: Left: 0.25", Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

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

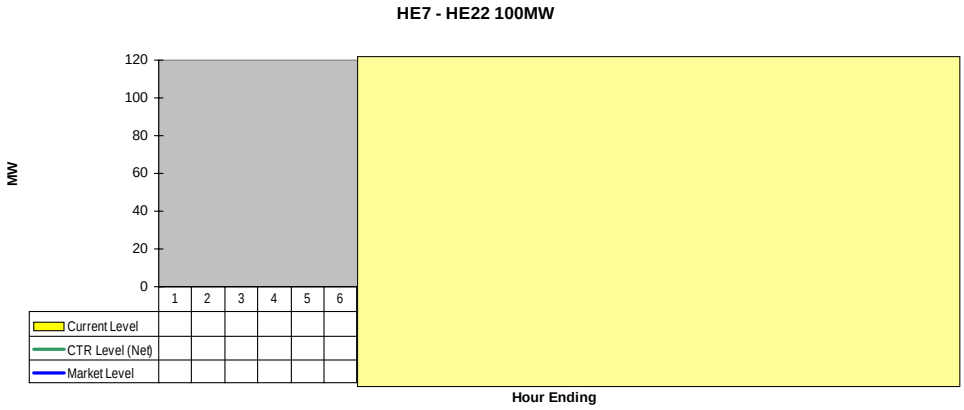
- The energy flow
- The maximum level at which the energy may reliably flow (default is unlimited)
- The transmission capacity committed to the transaction by the e-Tag Author as a Transmission Allocation

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.

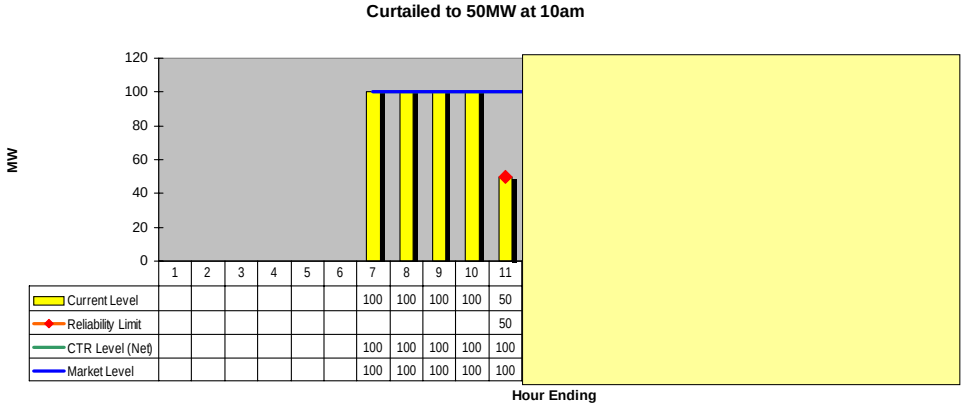
The following diagrams illustrate the relationship between these levels:

STEP 1 – New Tag Submission



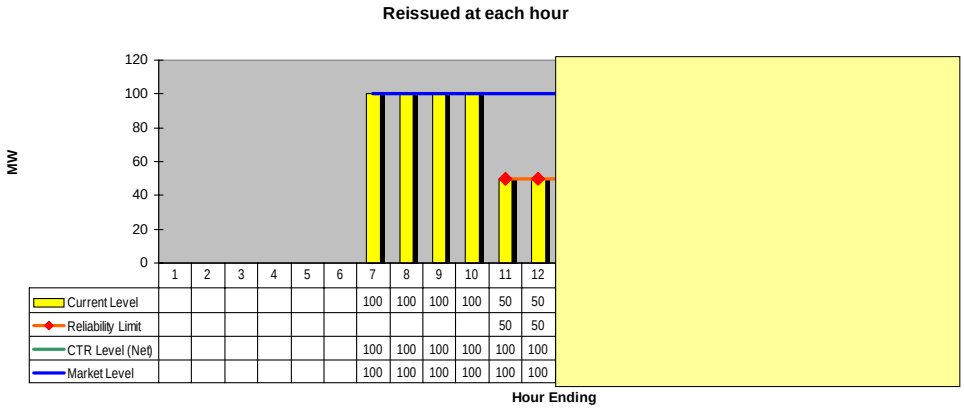
In Step 1, the e-Tag has been submitted, but has not yet run. The yellow overlay indicates points in the future.

STEP 2 – Curtailment



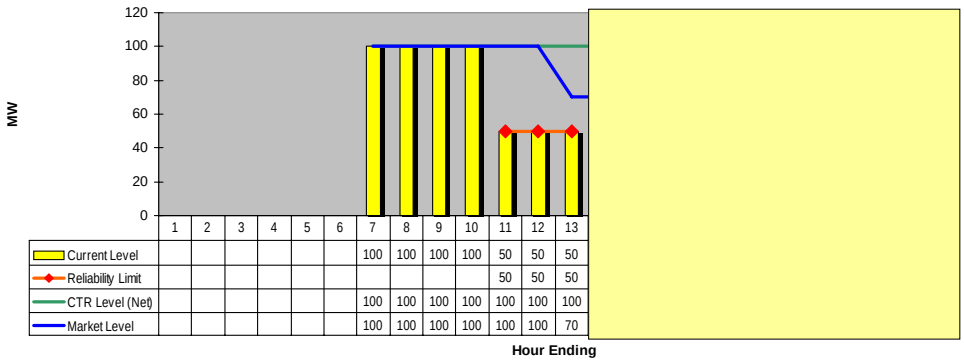
In Step 2, the e-Tag has been running and is curtailed.

STEP 3 – Curtailment Continues



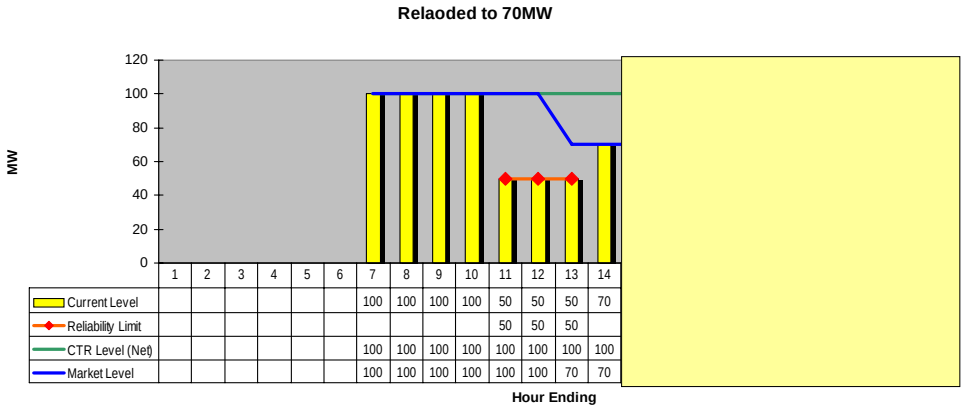
In Step 3, the Curtailment continues and is reissued twice.

STEP 4 – Tag Author Sets Reload Level



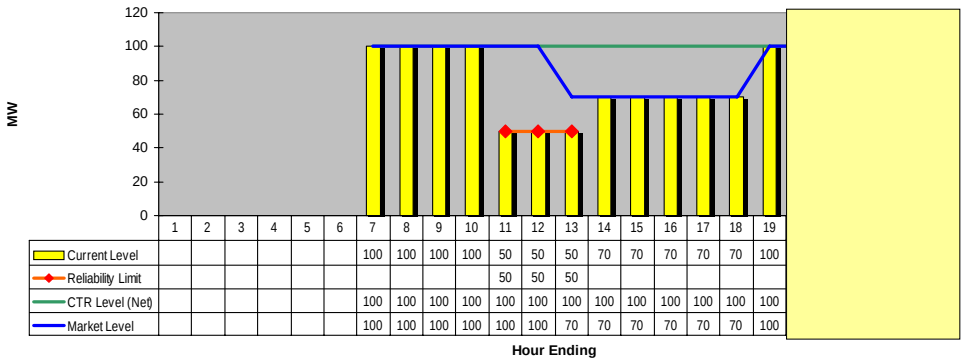
In Step 4, the e-Tag Author elects to limit their transaction to a maximum reload of 70MW until HE 18.

STEP 5 – TLR Released, Tag Partially Reloaded



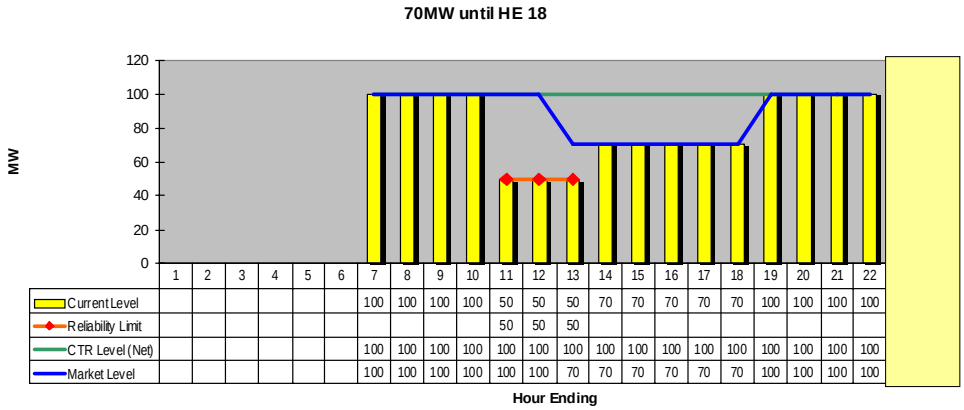
In step 5, the e-Tag is Reloaded by the RC/BA to the 70MW level as specified.

STEP 6 – Tag Fully Reloaded



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

STEP 7 – Transaction Complete

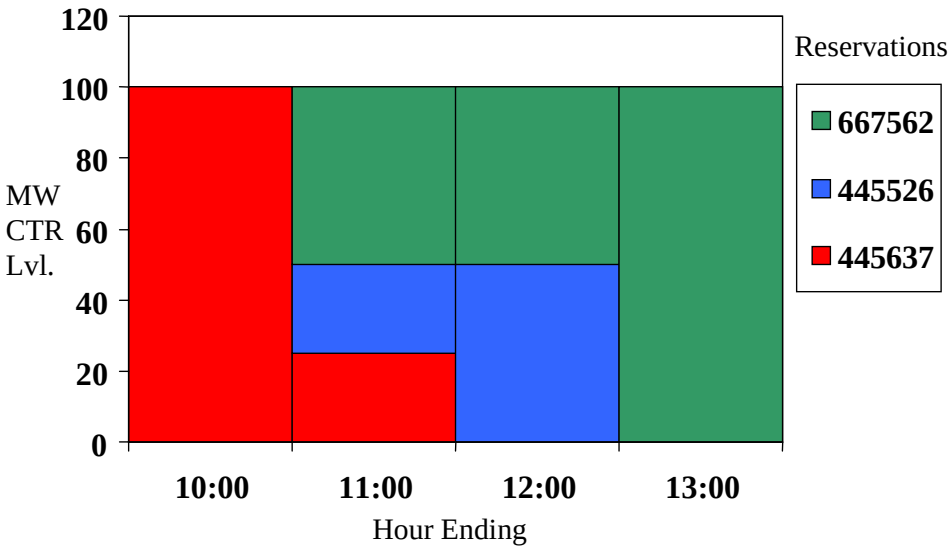


In Step 7, the e-Tag has completed.

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), as follows:

- These message dialogues need not be available for online query.
- Authority operators must have the ability to supply written reports listing message traffic for a particular entity or transaction within a reasonable amount of time (e.g., within seven business days).

Deleted: associated with a particular e-Tag

Deleted: .

Deleted: , however,

Formatted: Bullets and Numbering

Deleted: upon written request from NERC,

Deleted: be

Deleted: e

Deleted: one

Deleted: working week

Deleted: listing message traffic for a particular entity or transaction.

- Authority operators must retain message dialogues as specified in NERC/NAESB requirements.

Deleted: This information shall be kept

Deleted: from the implementation of the 1.7 Specification forward until such time this requirement is removed.

1.4.10 Rounding

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

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

1.4.11 Carbon Copy List

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

1.5 Training Requirements

1.5.1 User Guides

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

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

1.5.2 User Education

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

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

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

1.6 Functional Concepts

1.6.1 Initiating a Request

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

1.6.1.1 Submitting a New e-Tag Request

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

1.6.1.2 Submitting a Correction Request

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

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

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

1.6.1.3 Submitting a Profile Change Request

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

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

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

1.6.2 Request Distribution

1.6.2.1 Distributing a New e-Tag Request

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

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

1.6.2.2 Distributing a Correction Request

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

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

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

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

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

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

1.6.2.3 Distributing a Profile Change Request

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

1.6.3 E-Tag Request Actions

1.6.3.1 Approving and Denying Requests

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

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

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

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

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

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

1.6.3.2 Withdrawing a Request

For both New e-Tag Requests and Profile Change Requests, the Request initiator may withdraw the Request at any time up until the Request has reached a final state by submitting a WithdrawRequest message. If a Request has already been APPROVED, then that Request cannot be WITHDRAWN. In order to withdraw a Request, the initiator uses its Agent or Approval service 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 at the termination time and processed accordingly. The energy and transmission allocation profiles will be set to zero effective at the specified start time.

Should an entity wish to correct an invalid ATF e-Tag, that entity must submit a RequestTerminateTag. NERC/NAESB Standards describe the approval rights and responsibilities of the various entities involved in the approval process. If approved, the Composite State of the e-Tag is set to TERMINATED immediately 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 25 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.

Deleted: 24

1.6.5.2 Querying for an e-Tag

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

1.6.5.3 Querying for e-Tags

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

1.6.5.4 Querying for an e-Tag's History

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

1.6.5.5 Querying for Request IDs

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

1.6.5.6 Querying for a Specific Request

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

1.6.5.7 Querying for a Specific Request's State

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

1.6.5.8 Querying for Service Availability

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

Section 2 - Tag Agent Functional Requirements

2.1 Introduction

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

The Agent shall provide facilities to:

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

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

2.2 Registry Usage

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

2.3 Tag Data Entry and Viewing

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

2.3.1 Tag ID Creation

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

2.3.2 Security Key Creation

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

2.4 Date and Time Handling

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

2.5 Data Validation

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

2.6 Function Implementation

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

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

And process the following methods:

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

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

2.6.1 Initiating a Request

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

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

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

2.6.1.1 Submitting a New e-Tag Request

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

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

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

Formatted: Bullets and Numbering

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.
- Profile change requests may not add or remove any entity.

Formatted: Bullets and Numbering

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

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

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

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

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

2.6.2 Request Distribution

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

2.6.2.1 Processing a New e-Tag Request Distribution

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

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

2.6.2.2 Processing a Correction Request Distribution

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

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

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

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

2.6.2.3 Processing a Profile Change Request Distribution

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

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

2.6.3 Request Actions

2.6.3.1 Approving and Denying Requests

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

2.6.3.2 Withdrawing a Request

The following procedure should be used to withdraw a Request:

- Write the withdraw message and encode it in a valid XML format (as described by the latest e-Tag schema). The Message must include the following items:

- The Request ID provided by the Authority at the time the request was made.
- The original Security Key for the transaction that was used in the e-Tag Creation message.
-

Deleted: A reason that explains why the Withdrawal was made.

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

2.6.3.3 Cancelling an e-Tag

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

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

2.6.3.4 Terminating an e-Tag

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

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

2.6.4 Information Distribution

2.6.4.1 Processing a Request Approval State Distribution

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

- The e-Tag ID Referenced in the message must be one held by the Agent
- The Security Key presented must be identical to the original Security Key provided at the time the Agent transferred the New e-Tag Request to the Authority

- The rules described in the Data Model and Method Descriptions sections must not be violated

2.6.4.2 Processing a Request Resolution Distribution

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

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

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

2.6.4.3 Processing a Potential TLR Profile Change Distribution

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

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

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

2.6.5 Query Functions

2.6.5.1 Synchronous Queries

Synchronous Queries include the following:

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

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

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

2.6.5.1.1 Query for an e-Tag

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

2.6.5.1.2 Query for Request IDs

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

2.6.5.1.3 Query for a Request

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

2.6.5.1.4 Query for a Request's State

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

2.6.5.1.5 Querying for System Availability

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

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

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

2.6.5.2 Asynchronous Queries

Asynchronous Queries include the following:

- Query Summaries
- Query e-Tags
- Query History

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

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

2.6.5.2.1 Query Summaries

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

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

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

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

- The rules described in the Data Model and Method Descriptions section must not be violated
- The Range specified must not exceed twenty-five (25) hours. Authorities are only required to provide 25-hours of information in response to any single query.

Deleted: four

Deleted: 24

Deleted: 24

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

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

2.6.5.2.2 Query e-Tags

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

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

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

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

2.6.5.2.3 Query History

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

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

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

2.7 Availability and Performance

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

Section 3 - Tag Authority Functional Requirements

3.1 Introduction

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

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

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

3.2 Registry Usage

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

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

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

3.3 Tag Data Entry and Viewing

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

3.3.1 Approval State Override

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

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

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

3.3.2 Security Keys

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

3.4 Date and Time Handling

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

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

The Authority Service must calculate the latest approval time in order to determine when to end the approval period and set the final Request State of an e-Tag. The absolute date/time by which an e-Tag may be approved is calculated based on a combination of the NERC/NAESB timing ~~tables~~ 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.

Deleted: guidelines

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

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

3.5 Data Validation

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

3.6 Function Implementation

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

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

And process the following methods:

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

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

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

3.6.1 Initiating a Request

3.6.1.1 Processing a New e-Tag Request Submission

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

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

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

Formatted: Bullets and Numbering

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.

Deleted: ¶

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.

In addition, all messages must be sent to any forwarding URL registered to a PSE, BA, or TSP in the distribution list. These forwarded messages shall not impact the Delivery State of the associated entity.

Formatted: Space After: 6 pt

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

TAG ID	REQUEST ID	ENTITY CODE	SERVICE TYPE	SERVICE URL

3.6.1.2 Processing a Correction Request Submission

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

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

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

Approval State reset to PENDING and be informed of the change through Correction Request Distribution.

3.6.1.3 Processing a Profile Change Request Submission

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

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

Formatted: Bullets and Numbering

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

Profile changes to the Product Code or Transmission Allocation requires no approval process therefore ActOnByTime should be set to the time of receipt and TimeClassification should be set to "On Time".

If the Request changes the reliability limit, then the Authority must calculate the correct MW values to use for all profiles except for the source profile (which is included in the Profile Change message). The source profile will be associated with a physical location (BaseProfileID). If no physical location is included in the Profile Change message then the Authority will default the location to the GCA. The value of each profile calculated below must use the location information to calculate the correct profile values for both upstream and downstream profiles. The value of the profile at the physical segment specified in the Profile Change message will be the same as the source profile. The process for calculating upstream and downstream profiles is done in three steps: Loss Percentage, Carry Forward, and the New Limit calculation. The first step is to calculate the Loss percentage supplied by the creator of the original e-Tag based on the current MARKET LEVEL. This is done by applying the specified formula, for the day the curtailment is effective.

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

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

$$CarryForward_N = 0$$

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

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

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

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

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

Example:

Daily MWh POR = 100 MW
Daily MWh POD = 97 MW

SpecifiedLimit (Curtailed to) = 50 MW

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

$$CarryForward_{N0} = 0$$

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

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

Second Curtailment occurs to 40 MW

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

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

For PSE-Originating Market Changes:

For each supplied Exception Profile

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

Formatted: Indent: Left: 1.25", Bulleted + Level: 1 + Aligned at: 0.75" + Tab after: 1" + Indent at: 1", Tabs: Not at 1"

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.

Formatted: Indent: Left: 1.25", Bulleted + Level: 1 + Aligned at: 0.75" + Tab after: 1" + Indent at: 1", Tabs: Not at 1"

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,

Formatted: Indent: Left: 1.29", Bulleted + Level: 1 + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

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.

Deleted: ¶

Additional Implementation Details

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

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

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

Deleted: ¶

Formatted: Bullets and Numbering

3.6.2 Request Distribution

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

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

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

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

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

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

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

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

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

3.6.2.1 Distributing a New e-Tag Request

Deleted: ¶
¶
Formatted: Bullets and Numbering

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.

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
-

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

Deleted: 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:¶
<#>Any Entities being removed must be sent the correction with the impact flag set to TRUE¶
<#>Any Entities being removed must have their entries removed from the Distribution list¶
<#>Any Entities being removed must have their entries removed from the RequestApprovalRights list¶
<#>Any New Entities must have their entries added to the Distribution list¶
<#>Any new customers must have their entries added to the RequestApprovalRights list.¶
Following the completion of these steps, the Correction must be distributed normally.¶

Formatted: Bullets and Numbering

Deleted: The entity attempting to set State must have the most recent correction of the data within its scope

Deleted: Operator

- 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
-
- Withdraw Requests may be submitted for ATF Requests that have a Request State of PENDING

Deleted: A Withdrawal must be accompanied by a reason that explains why the Withdrawal was made.

Deleted: ¶

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.

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

WITHDRAWN is a final state.

3.6.3.3 Processing a Terminate Request

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

- The rules described in the Data Model and Method Descriptions sections must not be violated
- The e-Tag ID presented must represent an e-Tag currently held by the Authority
- The Security Key presented must be identical to the key associated with the Profile Change requester. For the e-Tag Author, this will be the Security Key presented to the Authority at the time the e-Tag was originally transferred by the Agent. For e-Tag Approvers, the key will be the Security Key assigned by the Authority at the time the new e-Tag was originally transferred to the Approval.
- RequestTerminateTag requests are only allowed for e-Tags that are CONFIRMED, IMPLEMENTED, or TERMINATED.
- The RequestTerminateTag request must contain a termination time that is between the e-Tag block start time and e-Tag block end time, and later than the time of receipt.
- A RequestTerminateTag request is invalid if it requests a start time that is later than or equal to an existing RequestTerminateTag Request for the same e-Tag; however, a request for an earlier termination time is allowable.
- Upon the RequestTerminateTag request becoming APPROVED, all PENDING RequestProfileChange requests with block end time after the termination time,

and all PENDING RequestTerminateTag requests with termination time after the APPROVED Request's termination time, must be set to a Request State of DENIED.

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

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

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

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

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.

Asynchronous responses must start within five minutes of query receipt.

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-five (25) hours. Systems may, at their option, reject any single query that indicates a desire for more than 25 hours of information.
- The rules described in the Data Model and Method Descriptions sections must not be violated

Deleted: four
Deleted: 24
Deleted: 24

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

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

3.6.5.2.2 Processing an e-Tags Query

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

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

Once a Query e-Tags message passes validation, the authority should return the requested data ordered by e-Tag creation time from oldest to most recent. Each callback message should contain one or more e-Tags, but not more than the number of e-Tags specified in the Return Rate field of the Query e-Tags message. Each message may contain fewer than the requested number of e-Tags. The security key used for the callback message should be the same security key that was used when the e-Tag Summary Query message was submitted.

3.6.5.2.3 Processing an e-Tag History Query

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

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

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

3.7 Availability and Performance

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

Section 4 - Tag Approval Functional Requirements

4.1 Introduction

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

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

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

4.2 Registry Usage

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

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

4.3 Tag Data Entry and Viewing

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

4.4 Date and Time Handling

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

4.5 Data Validation

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

4.6 Function Implementation

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

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

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeTerminateTag
- DistributeProfileChange
- DistributeStatus

- DistributeResolution
- CallbackSummaries
- CallbackTags
- CallbackHistory
- QueryAvailability

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

4.6.1 Initiating a Request

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

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

4.6.1.1 Submitting a Correction Request

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

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

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

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

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

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

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

4.6.1.2 Submitting a Profile Change Request

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

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

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

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

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

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

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

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

Formatted: Bullets and Numbering

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

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

4.6.2 Request Distribution

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

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

4.6.2.1 Processing a New e-Tag Request Distribution

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

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

4.6.2.2 Processing a Correction Request Distribution

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

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

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

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

4.6.2.3 Processing a Profile Change Request Distribution

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

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

4.6.3 Request Actions

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

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

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

4.6.3.1 Approving and Denying Request

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

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

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

Deleted: 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.
  -
- 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

Deleted: A reason that explains why the Withdrawal was made.

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-five (25) hours. Systems may, at their option, reject any single query that indicates a desire for more than 25-hours of information.

Deleted: four
Deleted: 24
Deleted: 24

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

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

4.6.5.2.2 Query e-Tags

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

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

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

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

4.6.5.2.3 Query History

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

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

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

4.7 Availability and Performance

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

Section 5 - Reliability Authority Service

5.1 Introduction

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

5.2 Registry Usage

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

5.3 e-Tag Data Entry and Viewing

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

5.4 Date and Time Handling

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

5.5 Data Validation

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

5.6 Function Implementation

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

- RequestProfileChange
- SetState
- DistributePotentialTLRProfileChange

And process the following methods:

- DistributeNewTag
- DistributeCorrection
- DistributeProfileChange
- DistributeResolution

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

5.6.1 Initiating a Request

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

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

5.6.1.1 Submitting a Profile Change Request

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

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

5.6.2 Request Distribution

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

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

5.6.2.1 Processing a New e-Tag Request Distribution

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

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

5.6.2.2 Processing a Correction Request Distribution

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

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

5.6.2.3 Processing a Profile Change Request Distribution

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

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

5.6.3 Information Distribution

5.6.3.1 Processing of a Request Resolution Distribution

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

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

5.6.3.2 Distribution of a Potential TLR Profile Change

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

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

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

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

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

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

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

5.7 Availability and Performance

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

Section 6 - Data Model Overview

6.1 Tag Data

6.1.1 Transaction Types

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

6.1.2 Market Segments

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

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

6.1.2.1 Scheduling Responsibilities

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

6.1.2.2 Title Transfers

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

6.1.3 Physical Segments

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

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

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

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

GPE: Generator
PSE: Transmission
LSE: Load

However, the following example is invalid:

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

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

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

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

Such cross references are invalid.

6.1.3.1 Generation

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

6.1.3.2 Transmission

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

6.1.3.2.1 Scheduling Entities

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

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

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

6.1.3.3 Load

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

6.1.4 Profile Sets

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

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

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

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

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

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

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

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

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

6.1.4.1 Profile Types

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

6.1.4.1.1 Market Level

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

6.1.4.1.2 Reliability Limit

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

6.1.4.1.3 Dynamic Minimum Energy

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

6.1.4.1.4 Dynamic Maximum Energy

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

6.1.4.1.5 Current Level

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

6.1.4.2 Profile Usage

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

6.1.4.2.1 Base Profiles

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

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

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

6.1.4.2.2 Exception Profiles

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

6.1.4.2.2.1 Market Level Exceptions

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

6.1.4.2.2.2 Reliability Limit Exceptions

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

6.1.5 Transmission Allocations

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

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

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

6.1.5.1 Base Allocation Profiles

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

6.1.5.2 Exception Allocation Profiles

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

6.1.6 Loss Accounting

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

Section 7 - Messaging Overview

7.1 Messaging Concepts

7.1.1 Use of the Transmission Control Protocol/Internet Protocol

The services defined in this document utilize the public Internet as their physical communication layer. Therefore, the underlying root protocol for this specification shall be TCP/IP. Utilization of HTTPS using NAESB PKI standard compliant certificates is required. The requirement for NAESB PKI standard compliant client certificates will 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, or any other port specified in the URL supplied in the registry, 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.

Deleted: based on

Deleted: is expected to

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

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

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

/~gads/meetings.html

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

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

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

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

7.1.1.1 Establishing Connections

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

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

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

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

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

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

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

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

7.1.1.1.1 Partial Connection Failures

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

A message shall be considered a duplicate if

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

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

7.1.1.1.2 Combining Messages

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

7.1.2 Use the Hypertext Transport Protocol

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

7.1.2.1 HTTP/S Requests

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

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

Content-length: <integer>

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

SOAPAction:NERCETag18:<method name>

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

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

7.1.2.2 HTTP/S Responses

HTTP Responses are returned to a client with the following syntax:
<HTTP Version> <State Code> <Explanation>
The State codes below are utilized and understood by the TIS services defined in this document:

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

Successful responses will be followed with an entity descriptor, describing the data to follow:
Content-type: text/xml
Declares that the type of data attached to the response will be an XML data set

Content-length: <integer>
Describes in bytes the length of the following attachment. The recipient uses this byte length to retrieve the Payload.

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

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

7.1.3 How SMXP Works

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

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

- The remote machine returns that document to the calling machine (again via HTTP).

Each SMXP method call has two important parts – the request and the response. Most of the methods used in e-Tag 1.7 are *synchronous* methods, meaning that once the calling machine makes a request, it waits for a response containing the results of its request before continuing.

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

7.1.4 Method Types

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

7.1.4.1 Requests

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

7.1.4.2 Request Distributions

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

7.1.4.3 Actions

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

7.1.4.4 Information Distributions

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

7.1.4.5 Queries

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

response contains the results of the query. Queries may be sent more than once for the same data, however, Queries sent more than five times for the same data may be rejected.

7.1.4.6 Callbacks

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

7.1.5 Faults

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

7.1.6 Return Values

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

7.1.7 Error Messages

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

7.2 Method Descriptions

The six fundamental method types align with the system concepts defined in Section 1 of this document. Those types are Requests, Request Distributions, Request Actions,

Information Distributions, Queries, etc. Details about the exact composition of these various data elements are defined in the latest e-Tag schema .

7.2.1 Special Data Structures

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

7.2.1.1 Tag ID

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

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

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

7.2.1.2 Message Info

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

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

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

7.2.1.3 Return State

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

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

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

7.2.1.4 Miscellaneous Info

In many messages, it is possible to communicate token/value pairs of non-standard information. This is included as a convenience and method for extending the e-Tagging system. By using the Miscellaneous Info function, entities can pass along data to other parties that is not directly supported by the data model. For example, when initiating a

curtailment request, an entity could provide various other information components, such as:
IMPACTED FLOWGATE : 1178
PROCEDURE : LLR
It is intended that entities make use of this feature in a standard, published manner that will allow recipients to process and utilize the information transferred.

7.2.2 Errors and Error Lists

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

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

0017	Missing DC Tie Operator	The RequestNewTag method cannot complete because a Balancing Authority registered to operate a requested DC Tie was not included as a Scheduling Entity for the Transmission Service Provider in the e-Tag.
0018	Orphan Profile	Every Profile must be reference by at least one Physical Segment
0019	Profile Not Found	The profile being referenced was not found in the e-Tag
0020	Invalid Path Order	The Market Segments, Physical Segments, and Parent market Segment References must be in correct order.
0021	Invalid Registered Value	A registered value is incorrect. This includes invalid or incorrect to/from entities, deactivated or unregistered PORs/PODs and/or Sources/Sinks, and non-existent products.

7.2.3 Initiating a Request

7.2.3.1 Special Data Structures

7.2.3.1.1 TimeClassification

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

7.2.3.2 Request New Tag

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

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

7.2.3.3 Request Correction

Issued by: Agents

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

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

7.2.3.4 Request Profile Change

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

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

7.2.4 Request Distribution

7.2.4.1 Special Data Structures

7.2.4.1.1 Approval Rights Flag

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

7.2.4.1.2 Impact Flag

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

7.2.4.2 Distribute New e-Tag

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

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

7.2.4.3 Distribute Correction

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

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

	0021 Invalid Registered Value

7.2.4.4 Distribute Profile Change

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

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

7.2.5 Request Actions

7.2.5.1 Set State

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

In	Message Info	Required
	Tag ID	Required
	Scope	Required
	Request Ref	Required
	Approval Status	Required
	Approval Time Stamp	
	Notes	Optional*
Out (successful)	ReturnState	
Errors	0002 e-Tag Not Found	

	0003 Segment not Found
	0005 Request Finalized
	0009 Invalid Security Key
	0013 Reason not Specified
	0016 Missing Correction
	0021 Invalid Registered Value

*Required for states of Denied or Study.

7.2.5.2 Withdraw Request

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

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

7.2.5.3 Terminate Request

Issued by: Agents, Approvals
Processed by: Authorities
Purpose: Used by request authors to set the transmission and energy profiles of an e-Tag to zero and set its state to TERMINATED after the request has transitioned to IMPLEMENTED. The Composite State of the e-Tag changes from IMPLEMENTED to TERMINATED once the current time is less than or equal to the termination time.

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	

Exhibit E

Modifications to WEQ-004

Modifications to WEQ-004 (New Requirements)

NOTE: NAESB Staff will assign appropriate enumeration to this standard to replace "n", with next sequential standard number within WEQ-004

NOTE: This section is a draft based on preliminary input from the JISWG

Coordinate Interchange for Capacity Benefit Margin

004-n All scheduled use of a Transmission Service Provider's transmission capacity set-aside for Capacity Benefit Margin (CBM) in support of energy imports into a load Balancing Authority served by the Transmission Service Provider shall be uniquely represented in all Requests For Interchange submitted to the IA.

004-n.1 Until other means for submitting the RFI are adopted by NAESB, the following data fields shall be specified in each e-Tag requesting the use of the Transmission Service Provider's CBM:

- The e-Tag transaction type shall be EMERGENCY
- The Transmission PSE (TPSE) listed in the physical segment where CBM is being requested shall be the registered Entity Code of the Load Serving Entity requesting use of CBM. Note that this is not necessarily the PSE submitting the e-Tag.
- The Transmission Product associated with the Transmission Service Provider whose use of CBM is being requested shall be 7-CB

004-n.2 The Transmission Service Provider may require the specification of a unique Transmission Reservation Number in association with any request for use of CBM. Such requirement shall be fully documented in the Transmission Service Provider's Business Practices posted on OASIS. The TSP reserves the right to deny any RFI requesting use of CBM if the required Transmission Reservation Number is not specified.