NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

February 8, 2001

Honorable David P. Boergers, Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Dear Secretary Boergers:

Open Access Same-Time Information System, Phase II
Docket No. RM00-10-000

Enclosed please find the original and 14 copies of the "Response of Electronic Scheduling Collaborative" to the advance notice of proposed rulemaking that the Commission issued in Docket No. RM00-10-000 on July 14, 2000.

Because the attachments to the Response are voluminous, we are submitting only 2 copies of the attachments. NERC has posted the entire filing, including attachments, on its web site (http://www.nerc.com/download/ferc_filings.html), which may be downloaded by clicking on "FERC-related Documents" under "NERC Fast Links." We are also sending an electronic copy of the entire filing informally to Commission staff.

Please acknowledge receipt of this filing by time stamping the additional copy and returning it to me in the enclosed preaddressed envelope. Questions about the filing should be directed to the undersigned. Thank you.

Sincerely,

David N. Cook
General Counsel

DNC:bsb
Enclosures

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Open Access Same-Time Information System, Phase II	))	Docket No. RM-00-10-000

RESPONSE OF ELECTRONIC SCHEDULING COLLABORATIVE TO ADVANCE NOTICE OF PROPOSED RULEMAKING

The Electronic Scheduling Collaborative ("ESC"), facilitated by the North American Electric Reliability Council ("NERC"), files this response to the advance notice of proposed rulemaking regarding OASIS Phase II that the Commission issued on July 14, 2000 ("the July 14 Notice").[1] In the July 14 notice the Commission requests:

> the submission of detailed proposals, by February 15, 2001, that will enable the Commission to adopt by regulation certain communications protocols and standards for business practices to implement Open Access Same-Time Information System (OASIS) Phase II. OASIS Phase II will be more functional than the current OASIS Phase IA, will incorporate electronic scheduling and will apply to the communications and related business practices between customers and Transmission Providers. * * * The comments and proposals submitted on February 15, 2001, should also propose an implementation schedule or plan to transition from OASIS Phase IA to OASIS Phase II, including time for testing, to allow the standards to be fully implemented by December 15, 2001. * * * The Commission intends to review the proposals received in response to the ANOPR and issue a Notice of Proposed Rulemaking (NOPR) or take other appropriate action.

NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. It works with all segments of the electric industry as well as customers to "keep the lights on" by developing and encouraging compliance with rules for the reliable operation of these systems. NERC comprises ten Regional Reliability Councils that account for virtually all

[1] *Open Access Same-Time Information System Phase II,* "Advance Notice of Proposed Rulemaking," 92 FERC ¶ 61,047, 65 *Fed. Reg.* 45,938 (July 26, 2000).

the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC convened the Electronic Scheduling Collaborative for the specific purpose of developing an industry response to the July 14 notice. The ESC is an open group with wide industry participation from all industry segments. One hundred eleven individuals from 65 companies and other organizations participated in the ESC. Attachment 1 to this filing identifies those individuals, organizations, and the ESC schedule of meetings. The ESC actively solicited participation from groups representing all segments of the industry, and the list of participants includes transmission providers, power marketers, independent system operators, transmission dependent utilities, Federal power marketing administrations, industry software developers, and other industry groups. NERC has posted all ESC minutes, documents and comments on a web page available to the public.[2] In addition, NERC maintains a list server for electronic scheduling that currently contains 338 subscribers from 161 different companies and organizations. The ESC has held two-day meetings each month since August 2000. Between meetings, the ESC has held conference calls, and several smaller task groups have developed background materials and draft papers for consideration of the entire ESC.

Once the ESC was established, a technical working group, known as the OASIS Standards Collaborative ("OSC"), was formed to work on the "how" of OASIS Phase II. The OSC is closely coordinating its efforts with those of the ESC. This filing includes documents that describe the status of the OSC's efforts to address the technical aspects of OASIS Phase II. The OSC is also an open group with wide industry participation. To date, 54 individuals from 35 different companies and other organizations have participated (see Attachment 2). The OSC list server currently contains 172 subscribers from 84 different companies and organizations.

Timetable

[2] http://www.nerc.com/~filez/eScheduling.html

Table 1 below is a timetable with a target for full implementation of OASIS Phase II. It calls for a consensus business practices document to be filed with the Commission in August 2001 and a consensus standards and communication protocols (S&CP) document to be filed with the Commission in December 2001. This timetable should enable full implementation of OASIS Phase II by Fall 2002, depending upon when the needed regulatory approvals are given and other operational constraints that affect implementation. It is the opinion of a strong majority of participants in the ESC and the OSC that full consensus implementation of OASIS Phase II by December 15, 2001 is not feasible.

OASIS Phase II promises significant improvements in the way industry participants do business with each other for both transmission and energy transactions, and those improvements should not be compromised by a rushed implementation. But the complexity of the undertaking and the need to still come to resolution of certain common business practice issues mean that the task cannot be completed in time (1) for the Commission to do a notice-and-comment rulemaking and (2) for companies to translate the outcome of that rulemaking into working software, all by December 15, 2001. To the extent feasible, the ESC will recommend to the Commission adoption of business practice standards that the ESC identifies as possible to institute prior to full implementation.

This timetable is based on the assumption that the ESC can achieve consensus on the remaining issues by the August filing. Participants in the ESC come from different market segments, have different business objectives, and are at different stages of development of their systems. That diversity results in a slow and laborious process to build consensus. If consensus should not be possible on certain issues, then the ESC will describe those issues in the August filing and request that the Commission resolve them. The time needed to resolve those issues may require adjustments to this schedule to incorporate any decisions into the final documents.

Projected Date	Milestones
15-Feb-01	Response to ANOPR
1-Mar-01	Implement OASIS S&CP Version 1.4
1-Apr-01	Final approval of E-Tag Version 1.7 Functional Specification
15-May-01	Post OASIS Phase II Business Practices and Functional Requirement Document for public comment
15-Jun-01	Comments on Business Practices due back
1-Aug-01	Finalize and File Business Practices Document for E-Scheduling / OASIS Phase II (ESC/MIC/OSC)
1-Oct-01	Implementation of E-Tag Version 1.7 (XML) to support RTO implementation
12/31/2001 (latest)	Finalize and file OASIS Phase II S&CP Document
	Software Development
	Regulatory approval needed before proceeding to Integration
	Integration with existing Scheduling processes in RTOs, CAs, SCs, TPs, PSEs, etc.
	Integrated testing of OASIS Phase II
	Training (2 to 3 Months minimum) for ALL Industry Participants
Fall 2002 *	Implement Full E-Scheduling / OASIS Phase II

The ESC requests that the Commission approve this proposed timetable for full implementation of OASIS Phase II. Relaxing the December 15, 2001 date will not jeopardize the Commission's intended start-up of regional transmission organizations. Those entities intending to participate in a regional transmission organization have, of necessity, already committed resources to developing their own systems for scheduling transactions as part of their efforts to be ready to do business by December 15, 2001. The Commission stated in Order 2000 that regional transmission organizations would have the responsibility to address interregional coordination by ensuring the integration of reliability practices within an Interconnection and market practices among Regions. Many of the proposed regional transmission organizations have participated in the ESC. Permitting the additional time for implementation of OASIS Phase II will actually enhance the ability of market participants to develop a fully functioning system for

electronic scheduling and will enable the industry to take advantage of newer technologies than are reflected in the current version of OASIS.

The implementation of OASIS Phase II will be based on open standards (meaning that interfaces will be clearly defined and non-proprietary). The ESC expects that those standards should enable RTOs to easily integrate with and expand upon their existing systems, to the extent possible, and should be considered in RTO systems under development. Existing RTO systems will bridge the gap between now and when OASIS Phase II is implemented. The open standards architecture of OASIS Phase II will mean that RTOs should be able to make significant use of their investment in existing systems. The ESC requests that, as the Commission acts on the pending RTO proposals, it place the clear expectation that RTOs will be required to be full participants in OASIS Phase II.

Background

At the time the Commission adopted its open access rule in Order No. 888, it also adopted a companion rule, Order No. 889, which required transmission providers to develop or participate in an electronic Open Access Same-Time Information System, or OASIS. Responding to industry comments, the Commission agreed that OASIS be implemented in two phases, with an initial phase to support exchange of basic transmission information and a second phase to support a fully functioning system with electronic scheduling of transactions. NERC facilitated an industry-wide OASIS "What" Group to develop the content and functionality for OASIS Phase I, and the Electric Power Research Institute facilitated an industry-wide OASIS "How" Working Group to develop the technical specifications for OASIS Phase I. The Commission subsequently adopted the work product from those two working groups as the basis for its detailed OASIS Phase I rules.

As open access transmission expanded, many utilities restructured their business operations and many new companies entered the growing competitive electricity markets. The number of transactions on the system and the complexity of those transactions have

grown enormously. Many in the industry felt a need to move to electronic scheduling of both transmission and energy transactions, for both commercial and reliability reasons. In early 2000, discussions began within NERC on what would be necessary to develop a fully functioning electronic scheduling system. NERC formed an Electronic Scheduling Task Force in April 2000 to continue those efforts. After the Commission issued its advance notice of proposed rulemaking in July 2000, NERC invited organizations representing the different segments of the electric industry to participate in the Electronic Scheduling Task Force. At the same time, NERC's Market Interface Committee recommended that the Electronic Scheduling Task Force be expanded to include representation from a broader cross-section of the industry. Thereafter NERC convened the Electronic Scheduling Collaborative to develop a response to the Commission's July 14 notice.

The procedures that the ESC would follow were simple. Membership and meetings were open to all interested persons. Documents, minutes, and comments would be publicly posted. The goal would be to achieve consensus on as many issues as possible. If votes were necessary, each person in attendance at a meeting would be permitted to vote. If consensus were not possible on a particular issue, the significant views of each position would be presented in the documents. The ESC would file its work product with the Commission and characterize it with whatever degree of consensus existed at the time of the filing.

Just as there was a need for a technical group to work on OASIS Phase I, an Electronic Scheduling How Working Group was established to respond to the "how" of OASIS Phase II. The group was a combination of NERC's Transaction Information Systems Working Group ("TISWG") and the OASIS How Working Group. The group subsequently changed its name to the OASIS Standards Collaborative ("OSC"). The OSC has drawn on the experience of the TISWG in E-Tagging and the OASIS How Working Group in its past work on OASIS and FERC filings to develop a cohesive technical portion for the industry's response to the July 14 notice.

NERC E-Tagging and OASIS Phase I presently are two separate systems that were not designed to communicate with each other. OASIS Phase II represents the merging of the tagging system, the transmission reservation system, and electronic scheduling into one cohesive system. To facilitate that merger, E-Tag Specification 1.7 and OASIS Phase II will use complimentary technology. Although E-Tag 1.7 does not include electronic scheduling, it will be a technological "stepping stone" on the way to full OASIS Phase II implementation.

Generator-Run Status

In the July 14 notice, the Commission asked if generator-run-status information should be incorporated into OASIS Phase II. NERC's Market Interface Committee and the ESC took formal votes on whether or not generator-run-status information should be publicly disclosed. Both groups voted overwhelmingly against disclosure (ESC: 2 votes in favor of disclosure, 24 votes against; MIC: 6 votes in favor of disclosure, 20 votes against), although a small minority continues to believe that generator-run-status information should be disclosed. To aid its deliberations, the ESC created two position papers on the issue and posted those papers for public comment. This filing includes those two papers and the comments from the public posting. On the basis of the MIC and ESC votes and the comments on the two position papers, the ESC believes there is a majority consensus in the industry not to disclose generator-run-status information.

Attachments to this Filing

This filing includes a number of draft documents developed by the ESC that together represent the current status of industry efforts to achieve consensus on OASIS Phase II:

- ESC Vision Statement (Attachment 3)
- Functional Requirements Document (Attachment 4)
- Business Practices Survey Summary (Attachment 5)
- Business Practices Development Summary (Attachment 6)
- Papers on Generator-Run Status (Attachment 7)

The following OSC draft documents are included as part of this filing. The substantive documents will be used to define a full Standards & Communication Protocols document.

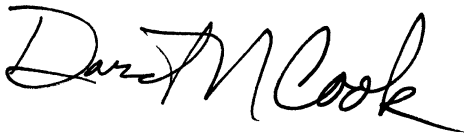
- OSC Scope Document (Attachment 8)
- Foundational Technologies Description (Attachment 9)
    - Simple Method eXchange Protocol and Style Guide 1.0
    - OASIS Security Requirements
    - Certificate Policy for Energy Market Access and Reliability Certificates (e-MARC)

Conclusion

The ESC and the OSC are well on the way to developing the business practices and standards and communication protocols for a fully functioning OASIS Phase II. Both the ESC and the OSC will continue their work, with a goal of meeting the proposed timetable. In particular, as stated in the timetable, the ESC anticipates filing a consensus business practices document in August 2001, and the OSC anticipates filing a consensus standards and communication protocols document in December 2001. These collaborative efforts will make it possible to develop the communications links and protocols needed to support electronic reservations and scheduling. A realistic assessment of the necessary steps for a consensus implementation of OASIS Phase II yields an achievable target of Fall 2002, depending on the time it takes to resolve any non-consensus issues and obtain the Commission's approval of the filings. The ESC requests that the Commission accept that schedule.

Submitted on behalf of the
Electronic Scheduling Collaborative

By the North American Electric
Reliability Council



David N. Cook
General Counsel

116-390 Village Boulevard
Princeton, NJ 08540-5731
(609) 452-8060
dcook@nerc.com

Attachment 1

Electronic Scheduling Task Force and ESC Meeting Schedule and Discussion Topics	
IOS Mini Workshop on Electronic Scheduling February 16, 2000 (Albuquerque, NM)	Brainstorming session on considerations of Electronic Scheduling
ESTF Meeting June 21, 2000 (Chicago, IL)	Appointed liaisons to work with to carry message and work with other NERC Groups
ESTF Conference Call July 18, 2000	Discuss FERC Advance NOPR. Many NOPR issues relate to the work of the ESTF especially: timing of the ESTF deliverable; developing a consensus among all industry participants; the scale and scope of the ESTF project. Issues surround the NOPR were delegated to the three ESTF Task Groups.
ESTF Meeting August 3–4, 2000 (Dallas, TX)	Discussed FERC's July 14 ANOPR for OASIS Phase II. Due to the issuance of the FERC ANOPR, the ESTF drafted statements to revise its role dealing with Electronic Scheduling.
ESTF Meeting September 13–14, 2000 (Cleveland, OH)	The ESTF passed three motions at its August 3–4 meeting dealing with the make-up of the ESTF, the charge that the ESTF make the ANOPR filing with FERC, and the process to be used in receiving input from NERC groups. Mike Gent, NERC President, wrote to the industry trade associations requesting their input into NERC's Electronic Scheduling efforts. The trade associations responded to Mr. Gent's letter and their response was also used by the TSC to provide guidance to the ESTF. Discussed proposed ES Model.
Electronic Scheduling – Request for Industry Participation September 20, 2000	In response to various industry group concerns regarding the formation and representation of the Electronic Scheduling Task Force, the North American Electric Reliability Council has formed an Electronic Scheduling Collaborative (ESC) to prepare a NERC filing in response to the FERC ANOPR (Docket No. RM00-10-000).
Electronic Scheduling Collaborative (ESC) Conference Call October 5, 2000	ESC reviews and revises Electronic Scheduling Vision Document, Functional Requirements Specification, and Data Exchange Model.
ESC Meeting October 23–24, 2000 (Denver, CO)	Discuss ESC presentation to NERC Board of Trustees. Presented the ESHOW report and discussed the recommendation that the TISWG, OASIS HOW, and ESHOW groups be combined into an OSC (OASIS Standards Collaborative). No structure or reporting relationship was recommended by the OSC. The OSC may also include IDCWG.
ESC Meeting November 8–9, 2000 (Las Vegas, NV)	Consulted FERC senior staff and clarified comments from the previous ESC meeting. FERC realizes that a set standard or business model is not possible for all RTOs. FERC does want as much commonality as possible when defining seams issues. Discussed ESC and CACTF Reliability Model.
Market Interface Committee Sponsors One-Day Work	The purpose of the workshop is to develop proposed positions on critical market interface issues in support of the Electronic Scheduling

Session "Critical Market Interface Issues in the Electronic Scheduling ANOPR" December 13, 2000 Washington, D.C.	Collaborative (ESC) response to the FERC ANOPR. See MIC "Related Files" on NERC web site: http://www.nerc.com/~filez/mic.html) Agenda for one-day work session "Critical Market Interface Issues in the Electronic Scheduling ANOPR" The MIC submitted comments to the ESC on the interface issues; the ESC responses to the MIC can found at: ftp://www.nerc.com/pub/sys/all_updl/oc/esched/esc-0101m.pdf
ESC Meeting December 20–21, 2000 (St. Louis)	Discussed Functional Requirements Document, Fragmented Scheduling Document. Reviewed latest work of OASIS Scheduling Collaborative. Discussed E-Tag 1.7 and Generation-Run Status Position Papers.
ESC Meeting January 18–19, 2001 (Atlanta, GA)	ESC and FERC meet on January 17 to discuss ESC documents to be filed for the OASIS Phase II ANOPR on February 15, 2001, the scope of the Electronic Scheduling effort, the continued work of the ESC after the filing date, and a timetable for completing that work.
February 6, 2001	Announce Implementation Dates for OASIS Phase II and E-Tag Version 1.7

ESC Participant List

First Name	Last Name	Company Name
Peg	Abbadini	CILCO
Chris	Advena	PJM Interconnection
Michael	Anderson	AEP Transmission
Dan	Baisden	SOCO
Ted	Bauman	Southern Company Energy Marketing
Stephen	Beuning	Xcel
Cindy	Blanchard	Cleco Power
Bert	Brehm	Altra Software
Shari	Brown	SPP
Bob	Burn	ABB
Kevin	Burns	OATI
Jim	Byrd	TXU
John	Calder	Dominion Virginia Power
David J.	Carlson	ComEd

Gerry	Cauley	NERC Staff
Dean	Chapman	NY ISO
Yilang	Chen	ABB
Scott	Cline	Reliant Energy
Steven	Cobb	SRP
Scott	Coe	BPA
Jack	Coleman	Unigrid Energy
Kurt	Conger	EXS for APPA
David	Cook	NERC Staff
Donnie	Cordell	Southeastern Power
Jason	Cox	Constellation
Phil	Cox	American Electric Power
Bob	Cummings	NERC Staff
Roger	Cummins	PsyCor
Jerry	Dempsey	WAPA
Ed	DeVarona	FPL/FRCC
Joel	Dison	SCG
Ed	Ditto	EMMT
Patrick	Doyle	TransEnergie, Hydro-Québec
Dave	Dworzak	EEI
Jim	Eckelkamp	CP&L
Gabriel	Ejebe	Siemens
Greg	Emery	OATI
Robert	Erbrick	El Paso Merchant Energy
Therese	Falcon	TransEnergy
Brett	Fisher	WAPA
Ryan	Fitz-Patrick	Constellation
Bill	Fredricksen	ComEd
Pete	Garris	California ISO
Jolene	Gleason	OATI
Jerry	Godwin	NIPSCO

Larry M.	Goins	TVA
Eric	Grant	CP&L
Jerry	Hagge	NPPD/MAPP
Michael	Hall	NCEMC
Jim	Hartwell	NPCC
Mark	Hecker	Entergy
Chris	Heschmeyer	Ameren Transmission
Dave	Hilt	NERC Staff
Peter	Hirsch	EPRI
Joe	Hopf	Ameren
Jim	Hudson	BPA – P
Will	Hurst	Louisville Gas & Electric Co.
Gary	Jackson	TVA
Grady	Kaough	Entergy
James	Killion	CILCO
Mike	Kormos (Chairman)	PJM
Monroe	Landrum	Southern Company/SERC
Michael	Leppitsch	APX
Kenneth	Lotterhos	NPCC
Steve	Lowe	Southern Co.
Mike	Martin	ALSTOM ESCA
Michael	McElhany	WAPA
Dave	McGinnis	Illinois Power
Bob	Merring	TVA
Melinda	Montgomery	Entergy
Don	Mooney	Southern Company
Chris	Moser	Dynegy Power Marketing
John G.	Mosier, Jr	NPCC
Tarek	Mourad	ABB Energy Information Systems
Talal	Murib	Southern Company
Benny	Naas	SIGECO

Mike	Oatts	Southern Co. Serv.
Christine	Ogozaly	DPL Energy Plus
Wayne Olfert	Olfert	Siemens
John	Paulsen	WAPA – LC
Wendell	Payne	Florida Power & Light Company
Dave	Perrino	APX
Dan	Prowse	Manitoba Hydro
Barbara	Rehman	BPA – T
Eric	Richer	ALSTOM ESCA
Rodney	Rienfeld	Dynegy
Andy	Rodriquez	Enron
Marvin	Rosenberg	FERC Staff
Kent	Saathoff	ERCOT
Jeff	Sand	Southern Co. Energy Mkt.
Mark	Scheel	Dynegy
Gordon	Scott	NERC Staff
Nathan	Sheik	Softsmiths
John	Simonelli	ISO New England
Jagjit	Singh	SRP
Bill	Smith	Allegheny Power
Paul	Sorensen	AEP
Bob	Steigmeier	Aquila Energy
Joe	Styslinger	Southern Company Generation
Dan	Tahija	California ISO
Anthony	Taylor	Williams Energy Marketing & Trading
Patt	Terris	PECO Power Team
Bill	Thompson	American Electric Power
Henry	Thompson	Entergy
Kalim R.	Tippitt	Reliant Energy
Paul	Turner	Georgia System Operations
John	Underhill	Salt River Project

Denis	Viau	Hydro–Québec
Tony	Vincik	NCEMC
Lydia	Vollmer	Exelon
Greg	Weiss	Ameren Energy
Knik	Whitney	Louisville Gas & Electric
Lisa	Wildes	PG&E Energy Trading
Louise	Witthuhn	FPC
Matt	Wolf	Entergy Transmission
Charles	Yeung	Enron Corp.
Dave	Zwergel	Midwest ISO

	Name of Company	E-Mail Address
1	ac.com	gregory.l.smith@ac.com
2	ac.com	james.b.broms@ac.com
3	adinet.com.uy	teixeirm@adinet.com.uy
4	aeci.org	baustin@aeci.org
5	aep.com	wrthompson@aep.com
6	aep.com	mcanderson@aep.com
7	aep.com	prsorenson@aep.com
8	aep.com	joemert@aep.com
9	aep.com	ftthomas@aep.com
10	aep.com	baondayko@aep.com
11	aep.com	jfstough@aep.com
12	AEP.COM	EPCOX@AEP.COM
13	alleghenypower.com	wsmith1@alleghenypower.com
14	alleghenypower.com	TGrabia@alleghenypower.com
15	allegrodevelopment.com	SWC@allegrodevelopment.com
16	alstom.esca.com	bruce.scott@alstom.esca.com
17	altra.com	msundsten@altra.com
18	altra.com	bert.brehm@altra.com
19	altra.com	andy.tritch@altra.com
20	ameren.com	BBURBA@ameren.com
21	ameren.com	PLADD@ameren.com
22	ameren.com	JKell@ameren.com
23	ameren.com	cheschmeyer@ameren.com
24	amerenenergy.com	jhopf@amerenenergy.com
25	AmerenEnergy.com	GWeiss@AmerenEnergy.com
26	amerenenergy.com	sterelmes@amerenenergy.com
27	APPAnet.org	amosher@APPAnet.org
28	apx.com	dperrino@apx.com
29	apx.com	rsamuelson@apx.com
30	avistacorp.com	Ken.Karki@avistacorp.com
31	BCHydro.bc.ca	Brett.Garrett@BCHydro.bc.ca
32	BCHydro.bc.ca	Nick.Snowdon@BCHydro.bc.ca
33	BCHydro.bc.ca	Laura.Letourneau@BCHydro.bc.ca
34	BCHydro.bc.ca	Keith.Wagner@BCHydro.bc.ca
35	bpa.gov	bmrehman@bpa.gov
36	bpa.gov	fjhalpin@bpa.gov
37	bpa.gov	remessinger@bpa.gov
38	bpa.gov	twkochheiser@bpa.gov
39	bpa.gov	jehudson@bpa.gov
40	bpa.gov	ccarpenter@bpa.gov
41	bpa.gov	erivier@bpa.gov
42	bpa.gov	sacoe@bpa.gov
43	bpa.gov	kmjohnson@bpa.gov
44	bridge.com	kelly.hettler@bridge.com
45	caiso.com	pgarris@caiso.com

	Name of Company	E-Mail Address
46	caiso.com	RSullivan@caiso.com
47	caiso.com	DTahija@caiso.com
48	caminus.com	ku@caminus.com
49	cassocorp.com	rhouse@cassocorp.com
50	chelanpud.org	mike@chelanpud.org
51	ci.seattle.wa.us	Doug.Rough@ci.seattle.wa.us
52	ci.tacoma.wa.us	jtaffe@ci.tacoma.wa.us
53	cilco.com	PAbbadini@cilco.com
54	Cinergy.com	gcecil@Cinergy.com
55	cinergy.com	amok@cinergy.com
56	cinergy.com	wyeager@cinergy.com
57	cleco.com	cindy.blanchard@cleco.com
58	cmpco.com	rhonda.poirier@cmpco.com
59	conectiv.com	Bill.Fehr@conectiv.com
60	conectiv.com	tim.jurco@conectiv.com
61	core.com	dfriend@core.com
62	cox.rr.com	spalmer@cox.rr.com
63	cplc.com	joann.su@cplc.com
64	cplc.com	james.eckelkamp@cplc.com
65	cplc.com	eric.grant@cplc.com
66	csu.org	sschaarschmidt@csu.org
67	dairynet.com	jby@dairynet.com
68	dakota.net	mcelhany@dakota.net
69	daytonpower.com	rullett@daytonpower.com
70	dcpud.org	cwagers@dcpud.org
71	dom.com	Jack_Kerr@dom.com
72	dom.com	John_Calder@dom.com
73	dplinc.com'	'ron.lewis@dplinc.com'
74	dps.state.ny.us	diane_barney@dps.state.ny.us
75	dteenergy.com	pruehsr@dteenergy.com
76	dteenergy.com	eizansa@dteenergy.com
77	dteenergy.com	chaoe@dteenergy.com
78	duke-energy.com	mfgildea@duke-energy.com
79	duke-energy.com	damcree@duke-energy.com
80	duke-energy.com	rknight@duke-energy.com
81	duke-energy.com	jasonmarshall@duke-energy.com
82	duke-energy.com	ckheisler@duke-energy.com
83	dwp.ci.la.ca.us	ptan@dwp.ci.la.ca.us
84	dynegy.com	rmri@dynegy.com
85	dynegy.com	wtbr@dynegy.com
86	dynegy.com	MASC@dynegy.com
87	dynegy.com	Chris.Moser@dynegy.com
88	eal.ab.ca	Rob.Baker@eal.ab.ca
89	eal.ab.ca	Katie.Johnson@eal.ab.ca
90	ec-power.com	cade.burks@ec-power.com

	Name of Company	E-Mail Address
91	edisonmission.com	editto@edisonmission.com
92	eei.org	ddworzak@eei.org
93	elcon.org	jhughes@elcon.org
94	emss.com	gwg@emss.com
95	enron.com	charles.yeung@enron.com
96	enron.com	andy.rodriquez@enron.com
97	entergy.com	hwolf@entergy.com
98	entergy.com	NSAINI@entergy.com
99	entergy.com	LTHORN2@entergy.com
100	entergy.com	mmontg3@entergy.com
101	entergy.com	edavis@entergy.com
102	entergy.com	dmcneil@entergy.com
103	entergy.com	kbhatti@entergy.com
104	entergy.com	hthomps@entergy.com
105	entergy.com	awelch@entergy.com
106	entergy.com	sboyki2@entergy.com
107	epenergy.com	erbrickb@epenergy.com
108	epri.com	phirsch@epri.com
109	epsa.org	mbennett@epsa.org
110	er.oge.com	henrywc@er.oge.com
111	ercot.com	ksaathoff@ercot.com
112	esca.com	Michael.MARTIN@esca.com
113	exeloncorp.com	timothy.pifko@exeloncorp.com
114	exeloncorp.com	william.fredricksen@exeloncorp.com
115	ferc.fed.us	marvin.rosenberg@ferc.fed.us
116	ferc.fed.us	paul.robb@ferc.fed.us
117	ferc.fed.us	donald.lekang@ferc.fed.us
118	firstenergycorp.com	rmkovacs@firstenergycorp.com
119	fortechsw.com	subhashp@fortechsw.com
120	fpc.com	l.witthuhn@fpc.com
121	fpc.com	LOUISE.L.WITTHUHN@fpc.com
122	fpl.com	Wendell_Payne@fpl.com
123	fpl.com	eduardo_devarona@fpl.com
124	fpl.com	Luke_Whiting@fpl.com
125	frcc.com	lcampbell@frcc.com
126	frcc.com	escott@frcc.com
127	FriedWire.com	StuartWright@FriedWire.com
128	gasoc.com	paul.turner@gasoc.com
129	gen.pge.com	Lisa.Wildes@gen.pge.com
130	gpsnet.com	steve@gpsnet.com
131	hesinet.com	lrigby@hesinet.com
132	hollandbpw.com	nuismer@hollandbpw.com
133	hollandbpw.com	vanfarow@hollandbpw.com
134	hotmail.com	philippe__roy@hotmail.com
135	hotmail.com	richer_e@hotmail.com

	Name of Company	E-Mail Address
136	hydro.mb.ca	dcprowse@hydro.mb.ca
137	hydro.mb.ca	ljkuczek@hydro.mb.ca
138	hydro.qc.ca	falcon.therese@hydro.qc.ca
139	hydro.qc.ca	doyle.patrick@hydro.qc.ca
140	hydro.qc.ca	Horisberger.Hans@hydro.qc.ca
141	hydro.qc.ca	hendren.geoffrey@hydro.qc.ca
142	hydro.qc.ca	Richard.Jean-Claude@hydro.qc.ca
143	hydro.qc.ca	Lalonde.Ronald@hydro.qc.ca
144	hydro.qc.ca	viau.denis@hydro.qc.ca
145	ieee.org	SCBrown@ieee.org
146	iit.edu	flueck@iit.edu
147	illinoispower.com	christopher_roth@illinoispower.com
148	illinoispower.com	dave_mcginnis@illinoispower.com
149	imea.org	dispatch@imea.org
150	iso-ne.com	jsimonelli@iso-ne.com
151	iso-ne.com	mzeoli@iso-ne.com
152	iso-ne.com	pharris@iso-ne.com
153	iso-ne.com	burbschat@iso-ne.com
154	iso-ne.com	fsaavedra@iso-ne.com
155	kcpl.com	Mike.Gammon@kcpl.com
156	kemaconsulting.com	jresek@kemaconsulting.com
157	kemaconsulting.com	mschrameyer@kemaconsulting.com
158	kemaconsulting.com	dhackett@kemaconsulting.com
159	kemaconsulting.com	jbucciero@kemaconsulting.com
160	ladwp.com	dkurow@ladwp.com
161	ladwp.com	rpentr@ladwp.com
162	ladwp.com	aromer@ladwp.com
163	lgeenergy.com	knik.whitney@lgeenergy.com
164	lgeenergy.com	tom.krebs@lgeenergy.com
165	lgeenergy.com	Will.Hurst@lgeenergy.com
166	mapp.org	wj.head@mapp.org
167	mepcc.com	moltanem@mepcc.com
168	mid.org	jamesm@mid.org
169	mid.org	jeffd@mid.org
170	midamerican.com	NDHammer@midamerican.com
171	midwestiso.org	TBilke@midwestiso.org
172	midwestiso.org	dzwergel@midwestiso.org
173	midwestiso.org	APhelps@midwestiso.org
174	midwestiso.org	jgardner@midwestiso.org
175	midwestiso.org	bnutter@midwestiso.org
176	midwestiso.org	bhopfensperger@midwestiso.org
177	mnpower.com	jmiller@mnpower.com
178	mrenergy.com	Jjerryt@mrenergy.com
179	nbpower.com	davedaley@nbpower.com
180	nbpower.com	nseely@nbpower.com

	Name of Company	E-Mail Address
181	ncemcs.com	michael.hall@ncemcs.com
182	nerc.com	barbara@nerc.com
183	nerc.com	gordon.scott@nerc.com
184	nerc.com	don.benjamin@nerc.com
185	nerc.com	gcauley@nerc.com
186	nerc.com	abonilla@nerc.com
187	NiagaraMohawk.com	hasenwinkeld@NiagaraMohawk.com
188	nipsco.com	clcrum@nipsco.com
189	nothnbut.net	steve537@nothnbut.net
190	npcc.org	npccrep@npcc.org
191	npcc.org	proman@npcc.org
192	npcc.org	jhartwell@npcc.org
193	nppd.com	jwhagge@nppd.com
194	nrgxs.com	kconger@nrgxs.com
195	NU.COM	zaklurc@NU.COM
196	nyiso.com	rgonzales@nyiso.com
197	nyiso.com	dchapman@nyiso.com
198	nyiso.com	ktammar@nyiso.com
199	nyiso.com	ftheadore@nyiso.com
200	oatiinc.com	kevin.burns@oatiinc.com
201	oatiinc.com	greg.emery@oatiinc.com
202	oatiinc.com	Sasan.Mokhtari@oatiinc.com
203	oatiinc.com	Ilya.Slutsker@oatiinc.com
204	oatiinc.com	Kevin.Sarkinen@oatiinc.com
205	oatiinc.com	Jolene.Gleason@oatiinc.com
206	oge.com	gunescj@oge.com
207	opc.com	PAUL.TURNER@opc.com
208	oppd.com	dkulisek@oppd.com
209	oppd.com	jiverson@oppd.com
210	otpco.com	lkittelson@otpco.com
211	ovec.com	bsquibb@ovec.com
212	pacificorp.com	byron.palmer@pacificorp.com
213	pacificorp.com	richard.bishop@pacificorp.com
214	pacificorp.com	ron.mccormick@pacificorp.com
215	pacifier.com	Barhitte@pacifier.com
216	peopleinthebox.com	brian.fihn@peopleinthebox.com
217	perot-nerc.com	gonzalc@perot-nerc.com
218	perot-nerc.com	porathb@perot-nerc.com
219	pgn.com	jd_ray@pgn.com
220	pgn.com	Bill_Casey@pgn.com
221	pgnmail.com	wayne.lewis@pgnmail.com
222	pjm.com	kormosmj@pjm.com
223	pjm.com	advena@pjm.com
224	pjm.com	Bresler@pjm.com
225	pjm.com	dadouria@pjm.com

	Name of Company	E-Mail Address
226	pjm.com	baizma@pjm.com
227	pjm.com	walton3@pjm.com
228	pnm.com	pnmoasis@pnm.com
229	pnm.com	jmontoy@pnm.com
230	powerex.com	phil.park@powerex.com
231	POWEREX.COM	MIKE.GOODENOUGH@POWEREX.COM
232	POWEREX.COM	IRENE.TOY@POWEREX.COM
233	powernav.com	vince@powernav.com
234	powerroots.com	nerc@powerroots.com
235	powersrc.com	jcox@powersrc.com
236	POWERSRC.COM	RFITZPAT@POWERSRC.COM
237	pplweb.com	jclambert@pplweb.com
238	pplweb.com	ceogozaly@pplweb.com
239	prpa.org	HarrisC@prpa.org
240	pseg.com	Brian.Krall@pseg.com
241	psycor.com	rcummins@psycor.com
242	psycor.com	smauser@psycor.com
243	ptialaska.net	ascc@ptialaska.net
244	puget.com	bharsh@puget.com
245	puget.com	pjones@puget.com
246	pwrteam.com	pterris@pwrteam.com
247	pwrteam.com	lvollmer@pwrteam.com
248	rapidnet.com	miketfr@rapidnet.com
249	reliantenergy.com	charles-bodden@reliantenergy.com
250	reliantenergy.com	Kalim_R_Tippitt@reliantenergy.com
251	reliantenergy.com	scline@reliantenergy.com
252	reliantenergy.com	kerrie_s_hlavaty@reliantenergy.com
253	santeecooper.com	jepeters@santeecooper.com
254	sbmu.net	dispatch@sbmu.net
255	scgo.com	kevin.lyons@scgo.com
256	scgo.com	david.shepheard@scgo.com
257	scsnet.com	Dan.W.Baisden@scsnet.com
258	sepa.doe.gov	bobg@sepa.doe.gov
259	sepa.doe.gov	DONNIEC@sepa.doe.gov
260	siemens-psc.com	wolfert@siemens-psc.com
261	siemens-psc.com	lcarter@siemens-psc.com
262	siemens-psc.com	jwaight@siemens-psc.com
263	siemens-psc.com	dtomasic@siemens-psc.com
264	siemens-psc.com	gejebe@siemens-psc.com
265	sisconet.com	john.gillerman@sisconet.com
266	sjlp.com	bcoker@sjlp.com
267	smmpa.org	ja.ihrke@smmpa.org
268	smud.org	pharrol@smud.org
269	snopud.com	wtmoojen@snopud.com
270	softsmiths.com	clazear@softsmiths.com

	Name of Company	E-Mail Address
271	softsmiths.com	lstone@softsmiths.com
272	softsmiths.com	nsheik@softsmiths.com
273	softsmiths.com	bPieri@softsmiths.com
274	southernco.com	mjlandru@southernco.com
275	southernco.com	JJDISON@southernco.com
276	southernco.com	dsmooney@southernco.com
277	southernco.com	SDLOWE@southernco.com
278	southernco.com	jwford@southernco.com
279	southernco.com	tbmurib@southernco.com
280	southernco.com	JRSTYSLI@southernco.com
281	southernenergy.com	ted.bauman@southernenergy.com
282	SouthernEnergy.Com	Jeff.Sand@SouthernEnergy.Com
283	splitrockenergy.com	BDEUTSCH@splitrockenergy.com
284	spp.org	sbrown@spp.org
285	spp.org	bgibson@spp.org
286	srp.gov	jtunderh@srp.gov
287	srpnet.com	sccobb@srpnet.com
288	srpnet.com	jxsingh@srpnet.com
289	tde.alstom.com	eric.richer@tde.alstom.com
290	theimo.com	ron.falsetti@theimo.com
291	theimo.com	kim.pitchell@theimo.com
292	theimo.com	roy.sepa@theimo.com
293	theimo.com	wayne.wong@theimo.com
294	tristategt.org	bsembrick@tristategt.org
295	tucsonelectric.com	chrisdickens@tucsonelectric.com
296	tva.gov	GWRudder@tva.gov
297	tva.gov	lmgoins@tva.gov
298	tva.gov	jpschwab@tva.gov
299	tva.gov	rlmerring@tva.gov
300	ucm.com	Steven.J.Hedden@ucm.com
301	ucm.com	Dennis.G.Friend@ucm.com
302	ucm.com	Joseph.P.Cook@ucm.com
303	ucm.com	christina.piazza@ucm.com
304	unigridenergy.com	jcoleman@unigridenergy.com
305	us.abb.com	tarek.mourad@us.abb.com
306	us.abb.com	elene.radinskaia@us.abb.com
307	us.abb.com	rajgopal.harnoor@us.abb.com
308	us.abb.com	bob.burn@us.abb.com
309	us.abb.com	vikram.janardhan@us.abb.com
310	us.abb.com	carlos.romero@us.abb.com
311	us.abb.com	bruce.siegel@us.abb.com
312	utilicorp.com	bsteigme@utilicorp.com
313	Vectren.com	MParsley@Vectren.com
314	vectren.com	bjn@vectren.com
315	wapa.gov	mcelhany@wapa.gov

	Name of Company	E-Mail Address
316	wapa.gov	goerger@wapa.gov
317	wapa.gov	rubbelke@wapa.gov
318	wapa.gov	HiedemanS@wapa.gov
319	wapa.gov	HUMBER@wapa.gov
320	wapa.gov	cass@wapa.gov
321	wapa.gov	croston@wapa.gov
322	wapa.gov	DEMPSEY@wapa.gov
323	wapa.gov	dake@wapa.gov
324	wapa.gov	Paulsen@wapa.gov
325	wapa.gov	crane@wapa.gov
326	wapa.gov	shiao@wapa.gov
327	wepco.com	rob.martin@wepco.com
328	wepco.com	Dianne.Palmen@wepco.com
329	wepco.com	marilyn.hartwig@wepco.com
330	williams.com	anthony.taylor@williams.com
331	Williams.com	Cherry.Smith@Williams.com
332	williams.com	tom.lehman@williams.com
333	wmcd.com	tnicholson@wmcd.com
334	worldnet.att.net	gcauley@worldnet.att.net
335	worldnet.att.net	tsaxton@worldnet.att.net
336	xcelenergy.com	Stephen.J.Beuning@xcelenergy.com
337	xcelenergy.com	sharon.r.miller@xcelenergy.com
338	XCELENERGY.COM	Robert.Weber@XCELENERGY.COM

1

Attachment 2

OASIS Scheduling Collaborative Meeting Schedule and Discussion Topics	
ESHOW October 18, 2000 Philadelphia, PA	Discussed FERC Advanced Notice of Proposed Rulemaking (A-NOPR) requiring a detailed proposal by February 15, 2001 and implementation by December 15, 2001, and ESTF/ESC Vision and Schedule.
TISWG November 1–3, 2000 Orlando, FL	1) NERC will inform the SCWG and CMWG that some people are still concerned that people do not understand approving tags when under TLR in order to facilitate reallocation. 2) Create some example for E-Tag SMXP. 3) Develop a straw man for E-Tag and OASIS security implementation in a timely fashion. 4) Develop data models in XML Schema for OASIS Phase II.
TISWG December 11–13, 2000 New Orleans, LA	*1)* NERC Updates 2) CACTF Update (Andy Rodriquez) 3) MIC/OC/PC Update (Andy Rodriquez) 4) TISWG Update (Andy Rodriquez) 5) Other miscellaneous updates (Brian Nolan) 6) ESC Update (Peter Hirsch/Andy Rodriquez) 7) OASIS XMLWG Report (Jagjit Singh, Todd Kochheiser) 8) Security Update (Todd Kochheiser) 9) XML Update (Todd Kochheiser) 10) Relation between E-Tag/E-Schedule and OASIS 11) How do the two relate? 12) Are we merging system, or making them talk to each other? OASIS Nodes exist independent of scheduling nodes OASIS Nodes are scheduling nodes 13) Merging of the S&CP with the E-Tag FS Document Overview of the E-Tag 1.7 Outline Overview of the S&CP Structure Merging Schemas and Data Dictionaries 14) Navigational paradigms? For informational postings? For GUIs?
TISWG January 9–11, 2001 Las Vegas, NV	1) Reissue security requirements and certificate policy documents 2) Draft OASIS Phase 2 S&CP outline 3) Draft tentative schedule for e-tag 1.7 specs/implementation 4) Draft tentative schedule for OASIS reservation/information: development of use-cases, development of object model, development of data model, development of SMXP methods and XML schema
OSC January 23–24, 2001 Houston, TX	ESC status report. Discussed E-Tag 1.7 implementation plan. Subgroup Status Reports and Data Modeling and Business Analysis for OASIS

OSC Participant List		
First Name	**Last Name**	**Company Name**
Aaron	Baizman	PJM
Alan	Thornton	Entergy
Allen	Phelps	MISO
Andy	Rodriquez	ENRON
Barbara	Rehman	BPA–T
Barbara	Zueco	ISONE
Bob	Barth	Cinergy
Bob	Cummings	NERC Staff
Brett	Fisher	WAPA
Brian	Lewis	OATI
Brian	Nolan	NERC Staff
Bruce	Urbshzt	ISO New England
Charles	Yeung	ENRON
Chris	Smant	PJM
Chris	Smith	CAISO
Corey	Rasmussen	OATI
Cory	Sellers	SWE
Dan	Baisden	SOCO
Don	Mooney	SOCO
Gabriel	Ejebe	Siemens
Ilya	Slutsker	OATI
Jagjit	Singh	SRP
Jerry	Dempsey	WAPA
Jerry	Hagge	NPPD
Jim	Eckelkamp	CP&L Marketing
Jim	Hudson	BPA
John	Calder	Virginia Power
John	Dadourian	PJM
John	Gillerman	SISCO
Karl	Tammar	NYISO
Larry	Gains	TVA
Laura	Polich	MAIN
Louise	Witthuhn	FPC
Mark	Scheel	Dynegy
Marv	Rosenberg	FERC Staff

Melinda	Montgomery	Entergy
Michael	Slater	SPP
Mike	Martin	Alstom ESCA
Mike	McElhany	WAPA
Nancy	Johnson	Allegheny Power
Paul	Sorenson	AEP
Peter	Hirsch	EPRI
Philippe	Roy	ESCA
Reynaldo	Bernal	Vitri
Sasan	Mokhtari	OATI
Shane	Eaker	SOCO
Sharon	Miller	Xcel Energy (IBM)
Talal	Murib	SOCO
Terry	Saxton	Xtensible Solution
Todd	Kochheiser	BPA–T
Vince	Wolodkin	POWERNAV
Wayne	Olfert	Siemens
Will	Briggs	Dynegy
William	Smith	Allegheny Power

OSC E-Mail Addresses		
	Company Name	**E-Mail Address**
1	aep.com	John_F._Stough@aep.com
2	aep.com	paul_r._sorenson@aep.com
3	aep.com	prsorenson@aep.com
4	alleghenypower.com	tgrabia@alleghenypower.com
5	alleghenypower.com	wsmith1@alleghenypower.com
6	allegrodevelopment.com	SWC@allegrodevelopment.com
7	allegrodevelopment.com	info@allegrodevelopment.com
8	alstom.esca.com	andrew.stanbury@alstom.esca.com
9	altra.com	DPhillips@altra.com
10	altra.com	MSundsten@altra.com
11	altra.com	atritch@altra.com
12	altra.com	bert.brehm@altra.com
13	ameren.com	BBURBA@ameren.com
14	ameren.com	JKell@ameren.com
15	ameren.com	frank_a_buchmeier@ameren.com
16	amerenenergy.com	gweiss@amerenenergy.com
17	ArcIT.com	InTENSE@ArcIT.com
18	bchydro.bc.ca	nick.snowdon@bchydro.bc.ca
19	bhe.com	bleeman@bhe.com
20	bpa.gov	bmrehman@bpa.gov
21	bpa.gov	jehudson@bpa.gov
22	bpa.gov	mewilczewski@bpa.gov
23	bpa.gov	twkochheiser@bpa.gov
24	bpa.gov	rgellingwood@bpa.gov
25	caiso.com	csmith@caiso.com
26	cassocorp.com	rhouse@cassocorp.com
27	cinergy.com	bbarth@cinergy.com
28	Cinergy.com	jpugh@Cinergy.com
29	cmpco.com	sggarwood@cmpco.com
30	cplc.com	james.eckelkamp@cplc.com
31	cplc.com	doug.white@cplc.com
32	cvps.com	bamelan@cvps.com
33	detroitedison.com	grabowskit@detroitedison.com
34	digsigtrust.com	alan.davidson@digsigtrust.com
35	dom.com	Don_Rumberger@dom.com
36	dom.com	Jack_Kerr@dom.com
37	dom.com	Jerry_Hubbell@dom.com
38	dom.com	John_Calder@dom.com
39	dom.com	john_calder@dom.com
40	doozer.com	barry@doozer.com
41	dplinc.com	thomas.senetra@dplinc.com
42	dynegy.com	Mark.Scheel@dynegy.com

43	dynegy.com	wtbr@dynegy.com
44	eaadvisors.com	ddaswani@eaadvisors.com
45	ecar.org	larryb@ecar.org
46	empros.com	wolfert@empros.com
47	emss.com	gwg@emss.com
48	emss.com	rsw@emss.com
49	emss.com	sje@emss.com
50	enron.com	andy.rodriquez@enron.com
51	entergy.com	lthorn2@entergy.com
52	entergy.com	mmontg3@entergy.com
53	epri.com	PHIRSCH@epri.com
54	epri.com	dbecker@epri.com
55	epri.com	phirsch@epri.com
56	esca.com	bindu.purhar@esca.com
57	esca.com	michael.martin@esca.com
58	esca.com	will.querdasi@esca.com
59	exeloncorp.com	timothy.pifko@exeloncorp.com
60	ferc.fed.us	marvin.rosenberg@ferc.fed.us
61	ferc.fed.us	william.booth@ferc.fed.us
62	firstenergycorp.com	jack_a._istvan@firstenergycorp.com
63	firstenergycorp.com	sensiusd@firstenergycorp.com
64	fortechsw.com	info@fortechsw.com
65	fpc.com	louise.l.witthuhn@fpc.com
66	fpl.com	ray_falcon@fpl.com
67	frcc.com	BarbaraD@frcc.com
68	frcc.com	bdoland@frcc.com
69	gpsnet.com	steve@gpsnet.com
70	gte.net	lstone@gte.net
71	hotmail.com	philippe__roy@hotmail.com
72	hotmail.com	richer_e@hotmail.com
73	hydro.mb.ca	dcprowse@hydro.mb.ca
74	hydro.qc.ca	falcon.therese@hydro.qc.ca
75	iso-ne.com	burbshat@iso-ne.com
76	iso-ne.com	bzucco@iso-ne.com
77	iso-ne.com	jsimonelli@iso-ne.com
78	iso-ne.com	fsaavedra@iso-ne.com
79	ix.netcom.com	fcleve@ix.netcom.com
80	maininc.org	lbp@maininc.org
81	mapp.org	ds.fredrickson@mapp.org
82	mapp.org	ta.anderson@mapp.org
83	midwestiso.org	aphelps@midwestiso.org
84	midwestiso.org	dzwergel@midwestiso.org
85	mplsconsult.com	mprickett@mplsconsult.com
86	nerc.com	glenda@nerc.com
87	nerc.com	bnolan@nerc.com

88	nerc.com	cummings@nerc.com
89	nerc.com	lcosta@nerc.com
90	nerc.com	lscott@nerc.com
91	nerc.com	tcampbel@nerc.com
92	nerc.com	gordon.scott@nerc.com
93	nerc.com	pjb@nerc.com
94	nevp.com	mmisra@nevp.com
95	nevp.com	torrey@nevp.com
96	niagaramohawk.com	hasenwinkeld@niagaramohawk.com
97	nppd.com	jwhagge@nppd.com
98	nsr.com	bvansant@nsr.com
99	nsr.com	cferguson@nsr.com
100	nsr.com	earellano@nsr.com
101	nsr.com	pburcky@nsr.com
102	nsr.com	vansant@nsr.com
103	nyiso.com	aelacqua@nyiso.com
104	nyiso.com	ktammar@nyiso.com
105	oatiinc.com	Guillermo.Irisarri@oatiinc.com
106	oatiinc.com	Ilya.Slutsker@oatiinc.com
107	oatiinc.com	Kevin.Burns@oatiinc.com
108	oatiinc.com	Nelson.Muller@oatiinc.com
109	oatiinc.com	chris.coyne@oatiinc.com
110	oatiinc.com	jolene.gleason@oatiinc.com
111	oatiinc.com	kevin.sarkinen@oatiinc.com
112	oatiinc.com	Brian.Lewis@oatiinc.com
113	ouc.com	gjackson@ouc.com
114	outhernco.com	mjlandru@southernco.com
115	pacificorp.com	byron.palmer@pacificorp.com
116	pacificorp.com	david.harries@pacificorp.com
117	pacificorp.com	richard.bishop@pacificorp.com
118	pacificorp.com	tarcy.lee@pacificorp.com
119	pgnmail.com	wayne.lewis@pgnmail.com
120	pgnmail.com	joann.su@pgnmail.com
121	pinnaclewest.com	michael.mraz@pinnaclewest.com
122	pjm.com	advena@pjm.com
123	pjm.com	baizma@pjm.com
124	pjm.com	mixsr@pjm.com
125	pjm.com	omalley@pjm.com
126	pjm.com	smart@pjm.com
127	pjm.com	bresler@pjm.com
128	pjm.com	dadouria@pjm.com
129	powernav.com	erne@powernav.com
130	powernav.com	vince@powernav.com
131	puget.com	bharsh@puget.com
132	pwrteam.com	lvollmer@pwrteam.com

133	pwrteam.com	EKrawiec@pwrteam.com
134	pwrteam.com	hyan@pwrteam.com
135	pwrteam.com	pterris@pwrteam.com
135	rapidnet.com	miketfr@rapidnet.com
137	reliantenergy.com	Kalim_R_Tippitt@reliantenergy.com
138	scsnet.com	don.s.mooney@scsnet.com
139	scsnet.com	dan.w.baisden@scsnet.com
140	siemens-psc.com	dtomasic@siemens-psc.com
141	siemens-psc.com	gejebe@siemens-psc.com
142	siemens-psc.com	skhatri@siemens-psc.com
143	siemens-psc.com	wolfert@siemens-psc.com
144	sisconet.com	john.gillerman@sisconet.com
145	softsmiths.com	nsheik@softsmiths.com
146	southernco.com	jjdison@southernco.com
147	southernco.com	jwviikin@southernco.com
148	southernco.com	mcseller@southernco.com
149	southernco.com	slsumral@southernco.com
150	southernco.com	tbmurib@southernco.com
151	southernco.com	jsgriffi@southernco.com
152	spp.org	cmonroe@spp.org
153	spp.org	jkeaton@spp.org
154	spp.org	bgibson@spp.org
155	spp.org	mslater@spp.org
156	srp.gov	jxsingh@srp.gov
157	srp.gov	tnnguyen@srp.gov
158	tecoenergy.com	axithier@tecoenergy.com
159	theIMO.com	ron.falsetti@theIMO.com
160	tva.gov	lwlundin@tva.gov
131	txu.com	ronhewlett@txu.com
162	us.abb.com	bruce.siegel@us.abb.com
163	ustra.mail.abb.com	dave.perrino@ustra.mail.abb.com
164	wapa.gov	dempsey@wapa.gov
165	wapa.gov	jbeasley@wapa.gov
166	wapa.gov	bfisher@wapa.gov
167	winfieldtech.com	kschmitz@winfieldtech.com
168	worldnet.att.net	gcauley@worldnet.att.net
169	worldnet.att.net	tdevaney@worldnet.att.net
170	worldnet.att.net	tsaxton@worldnet.att.net
171	xcelenergy.com	sharon.r.miller@xcelenergy.com

Attachment 3

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Electronic Scheduling Collaborative/ NERC Electronic Scheduling Task Force

ESC Vision Statement

January 25, 2001

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Electronic Scheduling Collaborative
Vision Statement

For business entities that operate in the electric utility industry, OASIS Phase II is a mechanism that will facilitate the scheduling of energy and transmission between marketing entities (PSEs, LSEs, GPEs, etc…), operating entities (traditional TPs, CAs, RTOs, ISOs, Generator Operators, etc…), and any grouping of the two. Unlike current processes, OASIS Phase II will provide a seamless method for interacting with and scheduling of transmission, ancillary services, and energy, regardless of region or operating entity. In addition OASIS Phase II will assist in Market Redispatch, provide TLR information and exchange reliability information to the Interchange Distribution Calculator.

OASIS Phase II must accomplish several objectives. Those objectives are:

- Facilitate Rights Tracking and Scheduling in a Timely Manner
- Accommodate Regional Diversity
- Ensure Reliable System Operations
- Provide Consistent Interfaces
- Function Consistently and Reliably
- Be Cost Effective

Facilitate Rights Tracking and Scheduling in a Timely Manner

First and foremost, OASIS Phase II must allow the tracking of rights to resources and scheduling of those rights to occur in a timely manner. New reservation requests, new schedules, schedule modifications, and schedule terminations/cancellations should be accomplished as quickly as possible from a commercial as well as reliability standpoint. In order to not limit responsiveness, OASIS Phase II must also allow for coordination and confirmation of schedules, as well as other functions, electronically and seamlessly between all parties within and between regions. Information should be shared and disseminated electronically and automatically, rather than through manual means (such as fax, telephone, e-mail). Information should also be either automatically or inherently verifiable. There should be no need to "check" a reservation or contract manually; an OASIS Phase II system should be capable of doing these checks automatically. All OASIS Phase II systems should allow for real-time status updates regarding current schedules/transactions, as well as historical audit and analysis of past transactions.

Accommodate Regional Diversity

OASIS Phase II should implement common business models when appropriate, but allow for both regional and market diversity and innovation. Various time frames, congestion management schemes, ramping rules, ancillary services, and uses of resources must be allowed. OASIS Phase II should also support various market models for the trading of transmission and energy, but in a manner that allows for exchange of common data to eliminate input redundancy.

Ensure Reliable System Operations

OASIS Phase II must also provide adequate information to support security analysis and reliability management. OASIS Phase II should provide for automated data exchange between operating entities and security coordinators, in order to provide accurate and up-to-date information allowing reliability entities the capability to evaluate the state of the electrical system. This information could also be used to provide the marketplace with tools to manage congestion on a forward or real-time basis.

Provide Consistent Interfaces

To ensure efficiency, OASIS Phase II systems must be developed with reasonably consistent interfaces (i.e., common nomenclatures, common data models, common navigational paradigms, etc…). The ability to transact business dealings through one apparent transaction ("one stop shopping") should be facilitated. Interfaces should be designed to meet the needs of a particular user base (i.e., marketers should have different interfaces than operating entities). Sufficient testing, training, and documentation must be developed and implemented.

Function Consistently and Reliably

OASIS Phase II systems must be reliable. Hardware and software systems must exist to ensure that the OASIS Phase II system is consistently available. Systems must be NERC standard compliant, tested, and correctly implemented prior to being allowed to participate as an OASIS Phase II system. Systems must also provide secure communications to ensure both the integrity of data exchange and positively identify scheduling participants.

Be Cost Effective

Finally, OASIS Phase II systems must be cost effective. If the defined requirements for OASIS Phase II make the provision of an OASIS Phase II system a barrier to market participation, we have not fully met the goals the FERC has put before us. In order to promote a cost effective transition from existing E-Tag and OASIS implementations, the use of components from existing systems should be evaluated wherever practical.

Next Steps

It is the vision of the Electronic Scheduling Collaborative to develop a set of functional requirements and associated Business Practices that standardize OASIS Phase II. Using these requirements as a basis, the OASIS Phase II Collaborative envisions the specification of a more detailed Standards and Communications Protocols document that defines standards for a common messaging system and a common data exchange model to be used by all OASIS Phase II participants. All electronic data exchanges between entities involved in the request, approval, implementation, and monitoring of transmission and energy rights and schedules shall occur on the basis of these standards. All data exchanges with existing systems (i.e. tagging, OASIS, proprietary scheduling systems, etc.) and future systems would be done based on these standards, possibly requiring the development of a "translation layer" between those existing systems and the OASIS Phase II system. Combined, the Functional Requirements, Business Practices, and Standards and Communications Protocol Document will be the basis for implementing OASIS Phase II across North America.

Attachment 4

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Electronic Scheduling Collaboration/ NERC Electronic Scheduling Task Force

OASIS Phase II Functional Requirements Specification

January 25, 2001

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Revision History

Date	Revision	Description	Author/Editor
September 17, 2000	0.9	Draft	Andy Rodriquez
October 5, 2000	0.91	Draft	Andy Rodriquez
October 31, 2000	0.92	Draft	Andy Rodriquez
November 9, 2000	0.93	Draft	Andy Rodriquez
November 29, 2000	0.94	Draft	Andy Rodriquez
January 25, 2001	0.95	Final	Andy Rodriquez

Table of Contents

1 Introduction 4
1.1 Vision Statement 4
1.2 Scope 5
1.3 ESTF/ESC Mission Statement 5
1.4 References 6
1.5 Assumptions and Dependencies 6
1.6 Definitions 6
2 Justification 7
2.1 Identified FERC Issues 7
2.2 Identified NERC Issues 7
2.3 Business Process 8
3 OASIS Phase II System Requirements 9
3.1 Functional Requirements 9
3.2 Non-Functional Requirements 10
3.2.1 Usability 10
3.2.2 Reliability and Security 11
3.2.3 Performance 11
3.2.4 Supportability 11
4 Design Considerations 11
5 Business Practice Issues 12
5.1 Identified Business Practices 12
5.1.1 Losses 12
5.1.2 Assignment of Responsibility 12
5.1.3 Regional Business Practices and Data Compatibility 12
5.1.4 Common Time Frames 12
5.1.5 Ancillary Services 13
6 Interfaces 13
6.1 User Interfaces 13
6.2 Hardware Interfaces 13
6.3 Software Interfaces 13
6.4 Communication Interfaces 13
6.4.1 System Layer 16
6.4.2 Communication Layer 16
6.4.3 Translation Layer 17
6.4.4 Common Translation Layers vs. Proprietary Translation Layers 17
7 Appendices 17
7.1 Background 17
7.2 Business Process Analysis 18
7.2.1 Actor List 18
7.2.1.1 Market Entity 18
7.2.1.2 Transmission Service Provider 19
7.2.1.3 Balancing Authority 19
7.2.1.4 Security Authority 19
7.2.1.5 Additional Actors 19
7.2.2 Current Business Process 19
7.2.2.1 Analysis 21
7.2.3 Proposed Business Process 21
7.2.3.1 Analysis 23
7.3 Issues Survey 24

1. Introduction

1.1 Vision Statement

For business entities that operate in the electric utility industry, OASIS Phase II is a mechanism that will facilitate the scheduling of energy and transmission between marketing entities (PSEs, LSEs, GPEs, etc…), operating entities (traditional TPs, CAs, RTOs, ISOs, Generator Operators, etc…), and any grouping of the two. Unlike current processes, OASIS Phase II will provide a seamless method for interacting with and scheduling of transmission, ancillary services, and energy, regardless of region or operating entity. In addition OASIS Phase II will assist in Market Redispatch, provide TLR information and exchange reliability information to the Interchange Distribution Calculator.

OASIS Phase II must accomplish several objectives. Those objectives are:

- Facilitate Rights Tracking and Scheduling in a Timely Manner
- Accommodate Regional Diversity
- Ensure Reliable System Operations
- Provide Consistent Interfaces
- Function Consistently and Reliably
- Be Cost Effective

Facilitate Rights Tracking and Scheduling in a Timely Manner

First and foremost, OASIS Phase II must allow the tracking of rights to resources and scheduling of those rights to occur in a timely manner. New reservation requests, new schedules, schedule modifications, and schedule terminations/cancellations should be accomplished as quickly as possible from a commercial as well as reliability standpoint. In order to not limit responsiveness, OASIS Phase II must also allow for coordination and confirmation of schedules, as well as other functions, electronically and seamlessly between all parties within and between regions. Information should be shared and disseminated electronically and automatically, rather than through manual means (such as fax, telephone, e-mail). Information should also be either automatically or inherently verifiable. There should be no need to "check" a reservation or contract manually; an OASIS Phase II system should be capable of doing these checks automatically. All OASIS Phase II systems should allow for real-time status updates regarding current schedules/transactions, as well as historical audit and analysis of past transactions.

Accommodate Regional Diversity

OASIS Phase II should implement common business models when appropriate, but allow for both regional and market diversity and innovation. Various time frames, congestion management schemes, ramping rules, ancillary services, and uses of resources must be allowed. OASIS Phase II should also support various market models for the trading of transmission and energy, but in a manner that allows for exchange of common data to eliminate input redundancy.

Ensure Reliable System Operations

OASIS Phase II must also provide adequate information to support security analysis and reliability management. OASIS Phase II should provide for automated data exchange between operating entities and security coordinators, in order to provide accurate and up-to-date information allowing reliability entities the capability to evaluate the state of the electrical

system. This information could also be used to provide the marketplace with tools to manage congestion on a forward or real-time basis.

Provide Consistent User Interfaces

To ensure efficiency, OASIS Phase II systems must be developed with reasonably consistent interfaces (i.e., common nomenclatures, common data models, common navigational paradigms, etc…). The ability to transact business dealings through one apparent transaction ("one stop shopping") should be facilitated. Interfaces should be designed to meet the needs of a particular user base (i.e., marketers should have different interfaces than operating entities). Sufficient testing, training, and documentation must be developed and implemented.

Function Consistently and Reliably

OASIS Phase II systems must be reliable. Hardware and software systems must exist to ensure that the OASIS Phase II system is consistently available. Systems must be NERC standard compliant, tested, and correctly implemented prior to being allowed to participate as an OASIS Phase II system. Systems must also provide secure communications to ensure both the integrity of data exchange and positively identify scheduling participants.

Be Cost Effective

Finally, OASIS Phase II systems must be cost effective. If the defined requirements for OASIS Phase II make the provision of an OASIS Phase II system a barrier to market participation, we have not fully met the goals the FERC has put before us. In order to promote a cost effective transition from existing E-Tag and OASIS implementations, the use of components from existing systems should be evaluated wherever practical.

1.2 Scope

The NERC Electronic Scheduling Task Force, in concert with the industry-representative Electronic Scheduling Collaborative, developed this document with two particular goals:

- Address the various problems and inefficiencies associated with the wholesale transactions of electric power
- Responding to the FERC's Advanced Notice of Proposed Rulemaking (ANOPR) regarding OASIS Phase II and Electronic Scheduling

As such, this document attempts to address the needs of the entire electric utility industry from both market and operational points of view.

1.3 ESTF/ESC Mission Statement

The Electronic Scheduling Collaborative shall define what is required to provide energy market participants with the capabilities to acquire transmission rights, schedule the intended use of those rights, and schedule the transport of energy and ancillary services seamlessly across control areas, regions and interconnections. The ESC shall also define what is required to provide Operating Entities (such as RTOs, CAs, and Security Coordinators load and generator operators) the ability to manage the electric system in times of normal economics, congestion, or emergency in an expeditious manner.

Objectives:

- Provide a consistent data model to allow communication across systems
- Be reasonably compatible with regional variations and flexible over time

- Preserve desirable benefits (e.g. reliability, marketing) of E-Tag System, IDC, OASIS, and proprietary systems
- Eliminate inefficiencies and redundancies in existing systems
- Optimize commonality in Business Practices and Data Requirements
- Electronic Scheduling should not be an incremental process to be performed in addition to existing scheduling and/or tagging processes, but should either be the result of and/or in lieu of existing scheduling/tagging processes.
- Minimize impact on existing ES systems, where they exist.

1.4 References

Data related to the ESC/ESTF and this work can be found at:

http://www.nerc.com/~oc/estf.html

Information related to OASIS can be found at:

http://www.tsin.com

Information related to the Control Area Criteria Task Force and their Reliability model can be found at:

http://www.nerc.com/~oc/cactf.html

For further information not listed in this document and not addressed above, please contact gordon.scott@nerc.com.

1.5 Assumptions and Dependencies

The FERC has imposed a deadline of February 15, 2001, for the definition of OASIS Phase II.
The FERC has required that industry-wide consensus be achieved with regard to OASIS Phase II. Where consensus is not achieved, we will provide differing opinions in the filing.
The ESC will coordinate development of OASIS Phase II with the CACTF and their reliability model.

1.6 Definitions

Electronic Scheduling – A process that will facilitate the processes of scheduling energy and transmission between Market Entities, operational entities (i.e., Transmission Service Providers and Balancing Authorities), and any grouping of the two.
Energy Schedule –The generation profile of an energy source with regard to a particular Transaction.
Load Schedule – The load profile of an energy sink with regard to a particular transaction.
Interchange Schedule – The planned transfer of energy between operational entities
Net Interchange Schedule – The summation of all interchange schedules between all operating entities.
One Stop Shopping – A mechanism to indicate a market desire to obtain necessary rights to support and schedule an entire Transaction through a single interface.
Tag – a document used to describe a Transaction for analysis.

Transaction –A collection of Energy, Load, and (if necessary) Transmission Schedules defining a path between operational entities.
Transmission Schedule – The planned usage profile for transmission rights to support a Transaction.

2. Justification

There are several reasons for implementing a new model for OASIS Phase II. This section describes the various issues and concerns that have been brought up with regard to OASIS and E-Tag that have led to the industry's desire to investigate changes to our current business model. These issues attempt to describe *problems,* and will later serve as a basis for determining functional requirements intended to fix those problems.

2.1 Identified FERC Issues

The following issues have been identified from FERC Docket No. RM00-10-000 Open Access Same Time Information System Phase II – Advance Notice of Proposed Rulemaking. These issues provide broad guidance regarding requirements for OASIS Phase II systems.
FI-1: The FERC believes standards must be developed for communications between Customers and RTOs to permit customers to expeditiously acquire common services among RTOs. These protocols would not standardize what the rights are, or the nature of the auctions. Instead, the focus of the communications protocols would be on how customers communicate their intentions to an RTO and how customers receive an RTO's responses.
FI-2: Since customers will often need to obtain transmission service across multiple RTOs, the FERC believes compatibility among RTOs with respect to transmission information and transaction requirements is essential.
FI-3: The FERC believes OASIS Phase II must facilitate communications between customers and Transmission Providers for services and critical market information e.g. auctions for transmission rights, posting of Available Transmission Capacity (ATC), total transmission capacity (TTC) and capacity benefit margin (CBM), prices for transmission and ancillary services, information on curtailments and interruptions and transmission facility status.
FI-4: The FERC believes OASIS Phase II should rely on the public Internet for communications
FI-5: The FERC believes OASIS Phase II should rely on World Wide Web browsers to provide interactive displays
FI-6: The FERC believes computer-to-computer communications should be accomplished through file upload/downloads.
FI-7: The FERC believes standard templates should be defined that facilitate the uploading/downloading of computer-to-computer communications.
FI-8: The FERC believes OASIS Phase II should incorporate Electronic Scheduling.
FI-9: The FERC requests discussion of the merits of including or excluding complete dynamic notification in OASIS Phase II.
FI-10: The FERC requests discussion of the merits of including or excluding generator-run status information in OASIS Phase II.
FI-11: The FERC requests identification of any business practices requiring standardization to facilitate the implementation of OASIS Phase II.

2.2 Identified NERC Issues

The members of the NERC Electronic Scheduling Task Force identified the following important issues that needed to be addressed by OASIS Phase II. These issues were taken from a longer

list of issues and identified as the top priority issues to be addressed. To see the complete list of issues and their rankings of importance, please see Appendix 7.3.

NI-1: Dealing with Curtailments
NI-2: Modifying a schedule after it has begun
NI-3: Correctly assigning responsibility to the proper entities
NI-4: Providing for the hourly market
NI-5: Incorporating scheduling timeframes (Hourly, daily, weekly)
NI-6: Offering electronic interchange schedule confirmation
NI-7: Incorporating automatic check out functions
NI-8: Dealing with Loss Accounting and Ancillary Services
NI-9: Having scheduling systems create tags for reliability monitoring
NI-10: Allowing the use of multiple transmission rights across time (horizontal stacking)
NI-11: Providing for in-kind losses
NI-12: Improving Operations Efficiency
NI-13: Reducing redundant data entry
NI-14: Providing a consistent interface to users
NI-15: Streamlining the market interface
NI-16: Mandating an industry-wide training program
NI-17: Offering "one-stop shopping" to market entities, (In the survey, One stop shopping was defined as the ability to provide (though internal or external development) a method in which one application can be used to schedule).
NI-18: Keeping operations free from market concerns
NI-19: Keeping the market free from operating concerns
NI-20: Permitting custom interfaces to accommodate regional needs
NI-21: Make the electronic scheduling system extremely reliable
NI-22: Requiring reliable networking, telecommunications, and computer hardware
NI-23: Designing to expand/extend functionality easily
NI-24: Making a fast process that can be automated extensively
NI-25: Make the electronic scheduling system cost-effective
NI-26: Providing the best electronic scheduling product possible
NI-27: Achieving majority stakeholder acceptance
NI-28: Implementing NERC-wide naming conventions
NI-29: Keeping systems simple and straightforward
NI-30: Integrating OASIS with scheduling
NI-31: Involving RTOs in the collaborative process
NI-32: Creating NERC-wide Scheduling Standards for Data Exchange
NI-33: Providing for entities internal to a Control Area (IPPs, etc.)/Offering tighter granularity in the scheduling process
NI-34: Designing the system to provide for different energy types
NI-35: Registering and formalizing business rules

2.3 Business Process

In addition to the above requirements, there are several inefficiencies associated with the current business process. These inefficiencies are based on both the need for users to interact with several different systems and manual interactions that allow for accidental corruption of information. For a detailed discussion of these issues and a proposal for a new structure to address these inefficiencies, please see Appendix 7.2.

3. OASIS Phase II System Requirements

The following requirements have been developed based on the NERC and FERC issues raised, the detailed analysis of the existing processes, and the proposed reorganization of those processes. These requirements are intended to resolve problems and issues identified in section 3. As such, references to issues are indicated in parenthesis so requirements can be traced back to original motivators. FERC issues FI-5, FI-6, and FI-7 are not referenced, as they relate primarily to the How (S&CP) requirements, which have yet to be defined.

3.1 Functional Requirements

Functional Requirements describe what the system must allow users to do. These items describe the most important features of the system.

FR-1: OASIS Phase II must allow schedules and changes to schedules (both market/transmission and operational/energy) to be requested and implemented as quickly as possible (from a reliability standpoint) by both customers and operational entities. (FI-8, NI-1, NI-2)

FR-2: OASIS Phase II must allow for the coordination and confirmation of schedules prior to implementation. (NI-6, NI-7, NI-12)

FR-3: OASIS Phase II must facilitate customer portfolio management of congestion (both predicative and real-time) through open and timely access to information. (FI-2, FI-3, FI-10, NI-1, NI-9,)

FR-4: OASIS Phase II must provide for coordinated dissemination of interchange schedules. (NI-6, NI-12)

FR-5: OASIS Phase II must allow reservation and scheduling of various attributes in an efficient yet explicit manner including but not limited to:

a. Hourly weekly monthly etc… (NI-4)
b. Flexible granularity (i.e., on the half, on the quarter, clock time, etc…) (NI-5)
c. Common time frames and common timing nomenclatures (on peak, off peak, etc…) (NI-5)
d. Varied ramping (at the top, across the top, varying durations, etc…)
e. Profiles
f. Product types (dynamic transfers, reserve sharing, market redispatch, etc.
g. Controlled interfaces (DC Ties, phase shifters)

FR-6: OASIS Phase II shall provide for verification of transmission and energy rights by providers as soon practical (possibly through automated means). (NI-12)

FR-7: OASIS Phase II shall allow involved parties to view and query information about transactions and reservations (such as statuses of schedules, schedules posted against reservations, use of versus remaining transmission rights etc…). (FI-3, FI-9, FI-10, NI-6, NI-7, NI-12)

FR-8: OASIS Phase II shall provide automated functions to allow operators with interchange schedules to confirm with adjacent control areas (current, next-hour, next-day, etc…). (NI-6, NI-12)

FR-9: OASIS Phase II shall provide automated functions to allow a means for schedulers from any entity to check their schedules with any other entity. (NI-6, NI-7, NI-12)

FR-10: OASIS Phase II shall provide tools for on-demand viewing of total net interchange schedules. (last hour, yesterday, last month, etc…). (NI-12)

FR-11: OASIS Phase II shall allow for the provision and scheduling of ancillary services. (NI-8)

FR-12: OASIS Phase II shall automatically provide reliability data to those operating entities responsible for security analysis. (NI-9)

FR-13: Flexible use of resources must be allowed, such as aggregation of generation, aggregation of load, and combinations of transmission rights in stacking (horizontal and vertical. (NI-10, NI-12)
FR-14: OASIS Phase II shall allow the scheduling of losses in kind. (NI-8, NI-11)
FR-15: OASIS Phase II shall accommodate regional business rules, as long as they do not conflict with OASIS Phase II's overall design goals, and aid in scheduling between regions. (NI-20)
FR-16: OASIS Phase II should accommodate the tracking of ownership of both transmission and energy (either through the inclusion of existing processes or the creation of new processes). (NI-8, NI-12, NI-30)
FR-17: OASIS Phase II should provide archiving and auditing capability.
FR-18: OASIS Phase II should allow for entities to store information related to their portion (or portions to which they have been given rights) of a transaction within that transaction (this information may be local or customized data).
FR-19: OASIS Phase II must provide a mechanism to support Generators, LSEs, and Transmission Rights Holders to approve transactions.
FR-20: OASIS Phase II must support all required functionality from OASIS Phase IA (version 1.4).
FR-21: OASIS Phase II must support all necessary functionality from Electronic Tagging.
FR-22: OASIS Phase II must provide real-time flows and limits on Critical Flowgates.

3.2 Non-Functional Requirements

Non-Functional Requirements describe items that are important to the systems development, but are not necessarily related to function. The system should have these requirements, but would function without them.

3.2.1 Usability

Usability Requirements describe those items related to the ease-of-use of the system. They are typically related to Functional Requirements, but do not define the functions themselves.
NFR-U1: OASIS Phase II shall allow all entities to respond to market or system needs as soon as practical. (NI-1, NI-2, NI-4, NI-12, NI-15)
NFR-U2: Duplicate data entry shall be eliminated. (NI-13)
NFR-U3: Interfaces shall have consistent "common nomenclatures, common data models, common navigational paradigms" from provider to provider, but not at the expense of innovation or functionality. Back office implementation of required functionality shall not be standardized unless specifically required (i.e., NERC wide ATC calculation methods, etc…). (NI-14, NI-15, NI-17)
NFR-U4: Interfaces shall be designed to provide regional diversity without compromising the consistent interface. (NI-14, NI-20)
NFR-U5: Functional roles, data requirements, and user interfaces shall be designed around the needs of the business entity (marketers, operators, etc…) using OASIS Phase II. (NI-15, NI-18, NI-19)
NFR-U6: OASIS Phase II shall be supported by training and documentation, to ensure people can indeed use OASIS Phase II as it was designed to be used. (NI-16)
NFR-U7: OASIS Phase II must support functionality to test and ensure real-time functionality without compromising system reliability. (NI-21)
NFR-U8: OASIS Phase II must allow users to view time-related information in the time zone of their choice.

3.2.2 Reliability and Security

Reliability Requirements describe the needs of the system with regard to up-time and continuous operation.
NFR-R1: OASIS Phase II systems must be available 24X7. (NI-21)
NFR-R2: Backup systems and procedures must be provided. (NI-21, NI-22)
NFR-R3: Data exchanges will use appropriate protocols to ensure reliable communication. (NI-21, NI-25)
NFR-R4: Security of data exchanges must be guaranteed. (NI-21)
NFR-R5: Business Entity and User identification and authentication must be supported. Users should be capable of being assigned one or more "roles" for a particular system.

3.2.3 Performance

Performance Requirements define how quickly or how accurately the system must be able to perform a certain task or set of tasks.
NFR-P1: OASIS Phase II systems must have measurable, adequate criteria for determining performance.
NFR-P2: OASIS Phase II systems must be S&CP compliant prior to and throughout operation of the system. (NI-21)

3.2.4 Supportability

Supportability Requirements describe how the system can be expanded upon or maintained.
NFR-S1: OASIS Phase II must be flexible enough to support changing data requirements. (NI-23)
NFR-S2: OASIS Phase II shall maximize configurability and modularization, so that system changes need not mean a complete system redesign. (NI-23, NI-25)

4. Design Considerations

Design Considerations attempt to identify issues that need to be addressed during the design process. While not necessarily related to the system functions, they are nonetheless important due to technology needs, pre-existing products, or other external forces.
DC-1: Cost of OASIS Phase II shall not be a barrier to market entry. (NI-25)
DC-2: In order to promote a cost effective transition from existing E-Tag and OASIS implementations, the use of components from existing systems should be evaluated wherever practical. (NI-25)
DC-3: User exposure to system complexity shall be minimized. (NI-29)
DC-4: OASIS Phase II must be tested, prototyped, and industry approved prior to release. (NI-25, NI-26, NI-27, NI-31)
DC-5: Industry participation shall be solicited at regular intervals in order to provide feedback. (NI-26, NI-27, NI-31)
DC-6: Industry updates and educational workshops shall be provided at regular intervals. (NI-16, NI-26, NI-27, NI-31)
DC-7: Data exchange standards and protocols must not limit business practices and data requirements:

a. Data exchange standards and nomenclature must be developed, published, and supported. (FI-1, FI-2, NI-28).
b. Data exchange standards and protocols must support various types of energy and transmission products. (NI-20, NI-34).

c. Data exchange standards and protocols must support scheduling granularity smaller than a control area. (NI-20, NI-33)
d. Data exchange standards and protocols must support various physical elements (i.e., Phase Shifting Transformers, DC Tie Lines, etc…). (NI-20)
e. Data exchange standards and protocols must be an open system (not proprietary or platform specific). (FI-1, NI-24, NI-29, NI-32)

DC-8: OASIS Phase II functionality shall be provided to the user through one apparent interface point. The location of the point (i.e., customer systems supplying the interface vs. provider systems supplying the interface) is currently irrelevant, but must be defined during the design process. (FI-3, NI-9, NI-13, NI-15, NI-17, NI-30)

5. Business Practice Issues

Some issues associated with OASIS Phase II are not technical in nature, but instead related to standardizing methods of dealing with certain situations or needs. These issues are identified in this section as Business Practices.

5.1 Identified Business Practices

During the Issues and Requirements Gathering Process, five primary Business Practice issues were discovered.

5.1.1 Losses

While the above requirements provide that OASIS Phase II must be capable of handling losses, we believe it is essential that all entities agree to some standard loss accounting methods and practices before OASIS Phase II can effectively address losses. The CACTF has proposed such a standard, which the ESC plans to follow if the standard is approved. (NI-8)

5.1.2 Assignment of Responsibility

The above requirements attempt to identify what OASIS Phase II can do, but not who is responsible for doing it. It will be extremely important to, through Policy, identify requirements and responsibilities of the different participants in the business process in such a manner that obligations are properly assigned and no ambiguity remains. The CACTF has proposed an assignment of those responsibilities to the various entities in the business process. The ESC plans to coordinate with the CACTF to ensure compatibility of OASIS Phase II design with those identified responsibilities. (NI-3)

5.1.3 Regional Business Practices and Data Compatibility

In order to ensure data compatibility, we feel one of the foundation steps for electronic scheduling will be to create a NERC-maintained "Data Dictionary," that describes various elements and/or formats for data. Once this catalog of requirements has been established, a data model can be defined and processes built around it. (FI-11, NI-32, NI-35)

5.1.4 Common Time Frames

As part of the examination of regional practices, some common time frames may be found to exist that would aid in understanding the needs of the market more fully. As such, we believe an important part of "common standards" will be the ability to define commonly used time frames for use in the data model and/or GUI. (NI-4, NI-5, NI-35)

5.1.5 Ancillary Services

Ancillary Services have not been discussed or addressed in detail yet. The development of Ancillary Service markets, and the definition of those Ancillary Services, must be considered.

6. Interfaces

The following sections describe the various interfaces that OASIS Phase II Systems will be required to support.

6.1 User Interfaces

User interfaces (i.e., screens seen and used by business entities) are expected to be varied among business entities. As such, there are no specific requirements with regard to user interfaces in this document. However, the following general statements can be made:

- All OASIS Phase II systems must allow for the viewing of “real-time” schedule information, as well as historical, planned, and summarized schedules (i.e., what is running now, what ran yesterday, what will run tomorrow, and a summary of the lifetime of the schedule).
- All OASIS Phase II systems should be capable of showing only “local” information, as well as more general information (i.e., show “my” schedule, as well as any overall schedule).
- All OASIS Phase II systems should use common nomenclatures, common data models, and common navigational paradigms in order to provide a consistent “look and feel” to all users.

It should be noted that no particular market model is being required or proposed. It is the goal of the ESC/ESTF to provide a flexible architecture that can support several different market models across a common communication mechanism, providing for regional diversity while at the same time allowing for increased efficiency through consolidation.

6.2 Hardware Interfaces

Hardware interfaces (i.e., physical machine connections to other resources, such as EMS systems) are expected to be varied among business entities. As such, there are no specific requirements with regard to hardware interfaces in this document.

6.3 Software Interfaces

Software interfaces (i.e., modifications to or inclusion of existing programs) are expected to be varied among business entities. As such, there are no specific requirements with regard to software interfaces in this document.

6.4 Communication Interfaces

It is expected that the implementation of standardized OASIS Phase II systems will require that the communications between the various systems will be done on a homogeneous basis using a consistent communications format and data exchange model. However, these systems currently support such communication in only a limited fashion. Existing systems will not be able to communicate with other systems without the development of "translation layers" that convert functions and data from proprietary systems into the homogeneous communication format and data exchange model. The result is a Layered Data Exchange Model as shown in Figure 6.4.

This diagram attempts to illustrate the manner in which systems will communicate utilizing the homogenous communication and data exchange protocols.

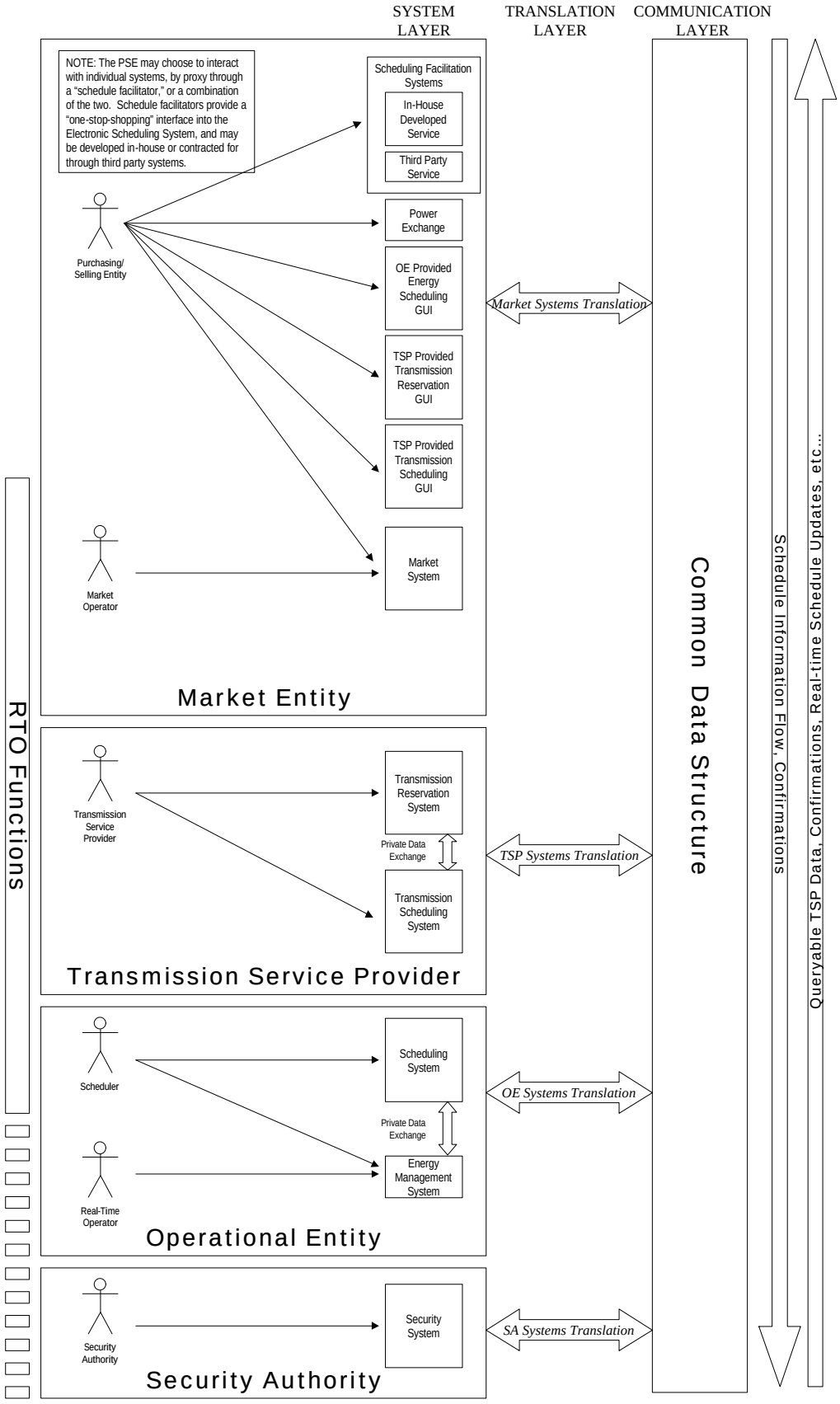


Fig 6.4 – Layered Data Exchange Model

This Layered Data Exchange Model concept facilitates the evolution, development, and enhancement of the wholesale power industry. With this model, systems may be added, deleted, replaced, or combined without affecting the interoperability of the whole as long as each new system conforms to the prescribed data exchange requirements and can appropriately submit requests to the Communication Layer.

6.4.1 System Layer

The System Layer consists of all existing and/or new systems required to perform the functions of OASIS Phase II. The systems shown in Figure 6.4 represents a sample of systems which may be required, but does not necessarily represent all systems which may be needed and/or required by OASIS Phase II. These systems may either be common (in that they are either provided to customers by the transmission provider or are provided by contractual agreement through a vendor) or proprietary (in that they are develop specifically by and for a particular entity). All systems at the System Layer will communicate with other systems at the System Layer through the Communication Layer via the Translation Layer.

6.4.2 Communication Layer

The Communication Layer represents the "least common denominator" for communications and data exchange. It is the intent that no system would communicate with another system without first going through the Communication Layer protocol. It is expected that the functionality of the Communication Layer will be such that any message submitted to the Communication Layer can be delivered to its intended recipient(s) without loss of functional intent or data content. Defined within this layer is a basic messaging and communications format to which all system-to-system communications must conform. While this does not specifically include the semantics of specific message definitions, it does include the format and syntax to which all messages should conform. Also defined within this layer is a common data structure that encompasses all foreseeable data requirements for electronic scheduling. While not all entities will utilize all aspects of the data model, the data model should be comprehensive enough to facilitate all data exchange requirements between systems. The Communications Layer is not itself a physical system, but rather a means for communicating between systems.

6.4.3 Translation Layer

The Translation Layer is used to convert all the functionality associated with the individual systems into the homogeneous communication format and data exchange model of the Communication Layer. The Translation Layer must contain translation routines to convert user actions into standardized messages from the system to other systems. The translation layer would generate and submit to the Communications Layer all necessary messages required to implement the functionality of the system. Likewise, the translation layer would receive all necessary messages delivered to it by other systems via the Communications Layer. The functional requirements associated with the translation layer for each identified system would contain all necessary details required to perform these functions. The translation layer may take one of many forms. The translation layer may be as simple as an algorithm contained within an existing legacy system or it may be as complex as a separate physical implementation providing translation services across the Internet to any number of existing or new systems. The Translation Layer would be developed and/or provided by users and/or vendors in accordance with the specified protocols.

6.4.4 Common Translation Layers vs. Proprietary Translation Layers

The functional requirements for the translation layers will be generically defined in the Electronic Scheduling Standards and Communications Protocol document for all system types. However, detailed design specifications for the translation layers for certain systems may be defined on a standardized basis due to the common nature of the system. Examples of common translation layers might include a translation layer for a generic, web-based PSE agent, transmission provider translation layers utilizing OASIS, and perhaps scheduling translation layers for those entities who currently schedule using the existing ETAG de-facto standard. However, certain proprietary PSE systems and control area scheduling systems may have to develop their own translation layers to interface to their existing legacy systems. These proprietary translation layers will be required to conform to the generic nature of the functional requirements of the translation layer associated with that system type.

7. Appendices

7.1 Background

The electrical energy industry, in the past four years has experienced dramatic, if not radical change. This current change was set in motion by FERC issuing Order 888 and 889. These Orders were written to facilitate open and unbiased access to the nations' transmission grid and encourage a separation of IOU generators from the wires business and customers.

In December 1999 FERC issued Order 2000. As stated in the summary of Order 2000, "The regulations require that each public utility that owns, operates, or controls facilities for the transmission of electric energy in interstate commerce make certain filings with respect to forming and participating in an RTO. The Commission also codifies minimum characteristics and functions that a transmission entity must satisfy in order to be considered an RTO. The Commission's goal is to promote efficiency in wholesale electricity markets and to ensure that electricity consumers pay the lowest price possible for reliable service."

Order 2000 also addressed existing entities such as PJM, NYISO and ISO-NE. FERC indirectly acknowledged wholesale trading inefficiencies that currently exist between these organizations

and urged a reduction in commercial seams: "We do not foreclose the possibility that an RTO may satisfy some of the minimum characteristics and functions by itself, while satisfying others through a strong cooperative agreement with neighboring RTOs to create a 'seamless trading area.' The functions of a large RTO may be met by eliminating the effect of seams separating smaller RTOs through a contract or other coordination arrangement."[1]

In addition to the FERC Orders 888/889 and 2000 there has been the release of an Advanced Notice Of Proposed Rulemaking (ANOPR) that instructs the industry to address the next phase of the Open Access Same-time Information System (OASIS). With the ANOPR the FERC is signaling to the industry, that it expects them to take OASIS to the next level in facilitating e-commerce by providing wholesale market participants with the capabilities for "one-stop" shopping; in other words, allowing participants the capabilities to electronically schedule transmission and energy into, out of, and across regional boundaries easily and seamlessly. To date, this capability does not exist. Furthermore, the industry itself is moving in this same direction through efforts within the North American Electric Reliability Council (NERC) structure. NERC has formed a group called the Energy Scheduling Collaborative/Electronic Scheduling Task Force ESC/ESTF. The charge of the ESC/ESTF is to define a system by which participants can conduct commerce almost seamlessly regardless of the type of transmission rights and congestion management implementations defined regionally.

7.2 Business Process Analysis

This section attempts to identify the basic business processes used today and illustrate where inefficiencies occur, with the goal of streamlining those processes in a manner that is beneficial to the industry.

7.2.1 Actor List

Actors define those entities that will use a system. The Control Area Criteria Task Force (CACTF) has identified several such entities with regard to Reliability and Control functions; this document uses those basic entities.

An actor does not necessarily represent an identifiable person or position; it instead refers to a particular business entity that encapsulates certain responsibilities and actions. These are general classes of responsibility. It should be noted that a business entity might function in more than one of these roles (for example, an IPP might function as both a Market Entity and a Operational Entity).

7.2.1.1 Market Entity

An entity that is eligible to purchase or sell energy or capacity and reserve transmission services, or any entity that acts to facilitate such transactions.
Examples: independent Marketer, Independent Power Producer (IPP) when selling energy, Transmission Dependent Utility (TDU) when purchasing services, Power Exchange.
Note: the CACTF defines three such entities: PSE, LSE, and Generator (Merchant). For the purposes of this document, these three entities have been combined as "Market Entities."

[1] FERC Order 2000, p258.

7.2.1.2 Transmission Service Provider

An entity that provides access to transmission service though provisions in a FERC-approved tariff.
Examples: Public Utility, Independent System Operator (ISO), Regional Transmission Organization (RTO), traditional Transmission Provider (TP).

7.2.1.3 Balancing Authority

An entity that coordinates energy transfers through the control of energy and/or control of load/generation balance.
Examples: Public Utility, Independent System Operator (ISO), Regional Transmission Organization (RTO), Generator Operator, traditional Control Area (CA).

7.2.1.4 Security Authority

An entity that monitors the transmission system in real-time and requests congestion management actions when necessary to maintain system integrity and reliability.

7.2.1.5 Additional Actors

Other actors exist that are not identified in this document (i.e., real-time operators, billing accountants, etc…). These actors are often contained within the entities defined above. For example, a real-time operator is an actor in the system defined by "Balancing Authority." A detailed analysis of the entity "Balancing Authority" might identify hundreds of different actors, and it is likely that those actors will vary from operational entity to operational entity (i.e., Southern Company might have different actors than Cinergy). However, for the purposes of OASIS Phase II, the actors within an entity or entity's system need not be defined.

7.2.2 Current Business Process

Figure 3.3.1 illustrates the current systems and processes used to arrange for and schedule energy and transmission today. Below the diagram are brief sentences that explain the meaning of the diagram.

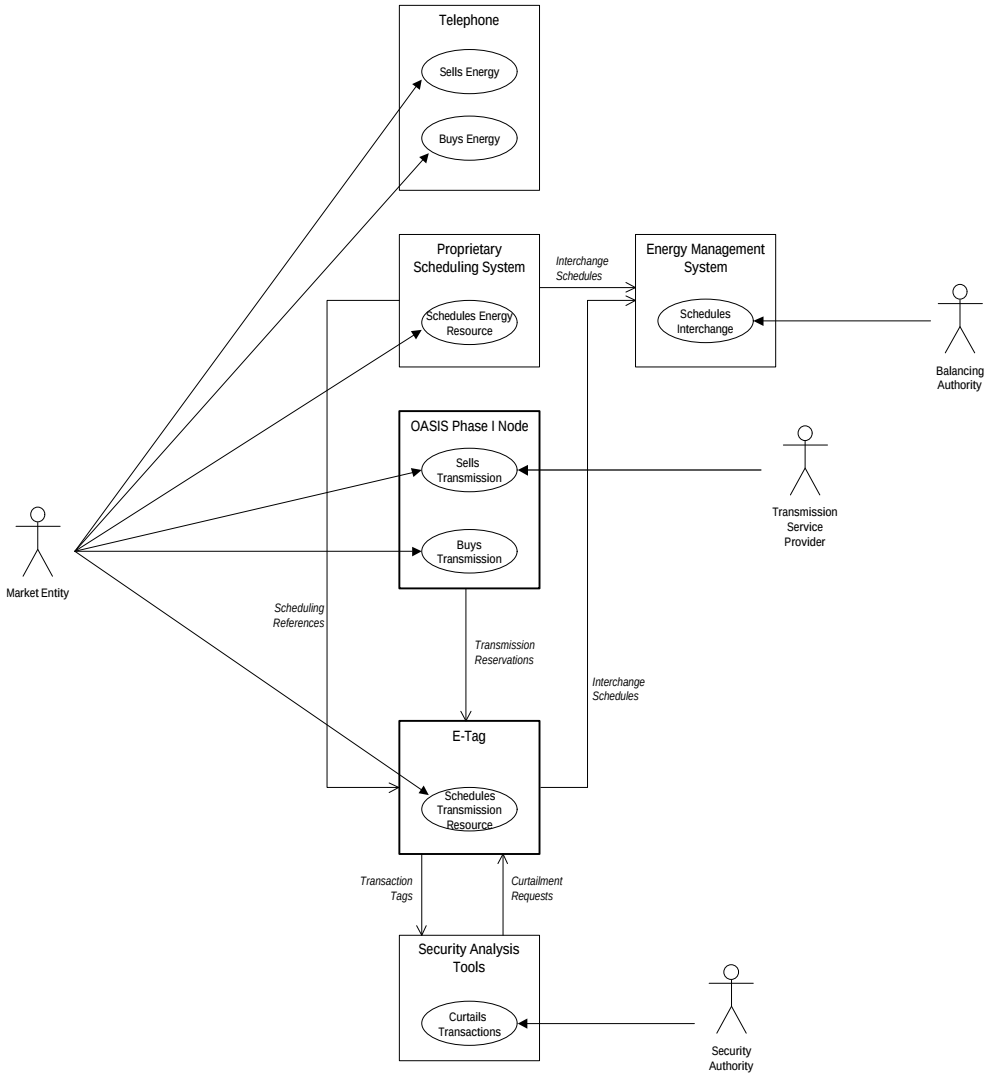


Figure 3.3.1

Market Entities
MEs use the telephone to buy energy.
MEs use the telephone to sell energy.
MEs use proprietary scheduling systems to schedule energy resources.
MEs use OASIS nodes to buy transmission rights.
MEs use OASIS nodes to sell transmission rights.
MEs use E-Tag to schedule transmission resources.

Transmission Service Providers
TSPs use OASIS nodes to sell transmission.

Balancing Authorities
BAs use EMS systems (populated with data data from proprietary scheduling systems and E-Tag) to schedule interchange.

Security Authorities
Security Authorities use the Security Analysis Tools and data from E-Tag to curtail transactions.

7.2.2.1 Analysis

The above diagram identifies several weaknesses of the current system that lead to inefficiencies.

1. Market Entities are required to deal with several different systems (telephone calls, proprietary scheduling systems, OASIS nodes, E-Tag). Even a simple transaction from one Control Area to a border CA requires several components (two phone calls, two interfaces with proprietary scheduling systems, two reservations on OASIS nodes, and an E-tag). This problem is referenced in both the NERC and FERC issues lists (FI-1, FI-2, NI-13, NI-14, NI-15, NI-17, NI-29, NI-30, NI-32).
2. Balancing Authority scheduling of Interchange is dependent on several different processes (proprietary scheduling systems scheduling the energy, OASIS nodes providing rights to necessary transmission, and confirmation of the transmission schedules through E-Tag) being completed and the information generated during that process being communicated to all involved parties. This non-integrated method of dependent processes makes it difficult to effectively coordinate interchange transactions. This problem is referenced in the NERC issues list (NI-2, NI-6, NI-7, NI-12, NI-18, NI-32).
3. Security Authorities are only involved with security analysis after all actions (buying/selling of energy, buying/selling of transmission, scheduling of energy, scheduling of transmission) have been completed. However, in order to reduce the need for reactive congestion management and offer more proactive reliability management tools, security analysis must occur before these actions are completed. The current model does not allow for any such analysis. This problem is referenced in the NERC issues list (NI-1, NI-9).
4. Controlled interfaces (DC Ties, Phase Shifters, etc…) are barriers to energy exchange. The existing electronic systems do not make adequate provision for describing schedules across such interfaces.
5. Benefits of the existing Business Model:
    a. In some regions, the existing OASIS and Electronic Tagging systems provide a means to reserve transmission service, schedule energy, and track energy flows. Industry participants continue to improve these systems; these improvements represent considerable investment, including automated transmission customer and provider back-end systems.
    b. Electronic tagging has improved reliability of transmission operations by providing transaction flow information to transmission reliability authorities for security analysis. This information is needed because of the parallel flow effects of most scheduled interchange.
    c. Electronic tagging has enabled Transmission Providers to process more transactions than would have otherwise been possible.
    d. For some Transmission Providers, the existing systems have enabled automation of checkout, billing, and transmission management processes.

7.2.3 Proposed Business Process

Figure 3.3.2 illustrates the proposed systems and processes used to arrange and schedule energy and transmission in the future.
It should be noted that the term “OASIS Phase II Node” is used in this proposed system to describe any FERC-approved market system for buying, selling, or scheduling energy and/or

transmission. An "OASIS Phase II node" could be an extension to an existing OASIS Phase IA node, a power exchange/trading hub system, a modification to an existing market system, or any other system, provided it meets the minimum data exchange standards defined in this document to allow for integrated OASIS Phase II functions. This would allow for the leveraging of existing legacy scheduling systems, given that their communication modules are modified to comply with the OASIS Phase II Standards & Communications Protocols document.
It should also be noted that the concepts of "energy" and "transmission" are purposefully ambiguous. The current system allows for some diversity in energy and transmission products. This flexibility must be carried forward and improved upon (i.e. "energy" may refer to PX transactions, dynamic schedules, and other diverse products other than the norm).

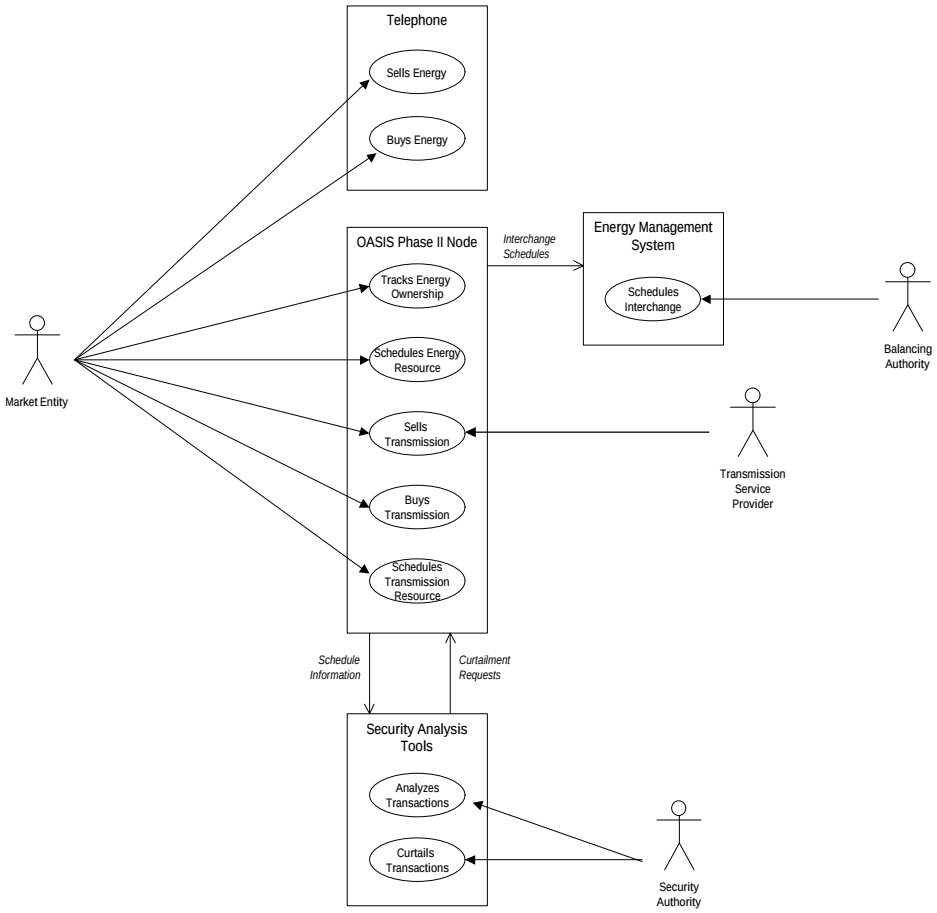


Figure 3.3.2

Market Entities
MEs use the telephone to buy energy.
MEs use the telephone to sell energy.
Mes use OASIS nodes to track energy ownership.

MEs use OASIS nodes to schedule energy resources.
MEs use OASIS nodes to buy transmission rights.
MEs use OASIS nodes to sell transmission rights.
MEs use OASIS nodes to schedule transmission resources.

Transmission Service Providers
TSPs use OASIS nodes to sell transmission.

Balancing Authorities
BAs use EMS systems (populated with data from OASIS nodes) to schedule interchange.

Security Authorities
Security Coordinators use Security Analysis Tools and data from OASIS nodes to analyze the transmission system.
Security Coordinators use Security Analysis Tools to curtail transactions.

7.2.3.1 Analysis

The system described above addresses the three problems identified in the previous analysis of the current business process:

1. Market Entities are no longer required to deal with several different systems. In the current business process, Market Entities are often required to deal with several different systems to complete the task of procuring and scheduling necessary resources to support a transaction. In the proposed process, the PSE is able to deal with one virtual system that provides access to all functions associated with a particular business entity (buying, selling, and scheduling energy and transmission).
2. Balancing Authorities are no longer dependent on the coordinated interaction of diverse systems. In the current business process, data exchange can sometimes be risky due to the various communications (both manual and electronic) required before a transaction becomes an implemented schedule. In the proposed process, interaction between systems is supported as an inherent design constraint, and as such, reduces the probability of error between systems.
3. Security Authorities are able to extract scheduling information at the time a schedule request is made, as opposed to the time a schedule is confirmed and implemented. In the current business process, source-to-sink transactions cannot be analyzed until the time they have been scheduled and committed to. In the proposed process, data can be extracted from OASIS systems in a more proactive manner, which in turn should lead to an earlier analysis of security conditions. This will allow a more proactive, flow-based security analysis to take place.

7.3 Issues Survey

Report of the Issues Task Team

July 29, 2000

Issues Survey – Description

The Issues Task Team developed a 68 question survey to aid in identifying important issues. This survey was based on the issues raised in the first ESTF meeting during the "introductions" portion of the meeting. These questions were posted on a web page where respondents could rank the issues by level of importance. A database server collected the data. At the completion of the survey period, the data was extracted and analyzed. Issues and data can be found at the end of this document.

Results of Issues Survey

Approximately 26 people responded to the survey (some participants elected to not answer some questions –all questions had between 24 and 26 respondents).

The data was collected over several days. Input was solicited from the membership of the ESTF.

Several general observations can be made based on the data collected:

- The Lowest Maximum for any given question answered was 9. This would seem to indicate that every issue listed in the survey was considered a top priority by at least one respondent.
- Most of the Highest Minimums for questions all occurred in the top 15 ranked questions, indicating that the everyone believed these issues to be at least of a moderate importance.
- The lowest mean rating for any given question was 3.792, indicating that the majority of the survey respondents felt even the least important issue had some importance.
- The top 24 issues had both high means and high modes, indicating a high level of consensus between respondents

Items of Importance

In summary, it would appear that the majority of respondents are concerned with system reliability and usability. System outages must be mitigated through the use of redundancy and technology. Tagging, OASIS, and proprietary scheduling systems have pointed to the fact that complex and diverse systems create confusion and difficulty. New systems should be easier to use, consistent, and more streamlined. Training programs are a must. Systems should leverage technology to assist in tedious and repetitive tasks, such as checkouts and data entry. All parties (PSEs, CAs, TPs, IPPs, etc…) should be involved in the process, pull their own weight, and have defined areas of responsibility. Changing issues, such as RTO formation, Interconnected Operations Services and Congestion Management, must be addressed. Perhaps most importantly, we should not rush into any quick solutions, but take time to properly develop the system.

The above summary was developed based on the below highly ranked issues. Exact statistical data values are listed at the end of this document.

- Making the electronic scheduling system extremely reliable and cost-effective
  - Confidence that the system works
  - 7x24, backed up, confirmed delivery
  - Defined performance measures
  - Requiring reliable networking, telecommunications, and computer hardware
  - Data exchange is secure and error-free
- Notification, confirmation, and implementation of schedules
  - Implementing schedules
  - Modifying schedules
  - Curtailing Schedules
- Improving Operations Efficiency\
- Reducing redundant data entry
- Correctly assigning responsibility to the proper entities
- Providing for the hourly market
- Providing a consistent interface to users
- Providing the best electronic scheduling product possible
- Designing to expand/extend functionality easily
- Achieving majority stakeholder acceptance
- Implementing NERC Wide naming conventions
- Incorporating automatic check out functions
- Incorporating scheduling timeframes (Hourly, daily, weekly)
- Making a fast process that can be automated extensively
- Keeping systems simple and straightforward
- Integrating OASIS with scheduling
- Streamlining the market interface
- Dealing with Loss Accounting and Ancillary Services
- Involving RTOs in the collaborative process
- Having scheduling systems create tags for reliability monitoring
- Mandating and industry wide training program

Items for Discussion

Several issues were identified for further discussion. These items did were not ranked with a high mean score, but had a high mode score, indicating that while the majority did not feel they were the most important, several people did feel that they were so. In order to ensure fairness, the Issues Task Team feels that these issues should be discussed further.

- Creating NERC Wide Scheduling Standards – There was some question as to the interpretation of this issue. When we say "Scheduling Standards," do we refer to common methods for exchanging data? Or do we refer to the more grandiose concept of standards for ramping, scheduling deadlines, etc…?

Data exchange must be standardized.
Other standards should be explored? But is not a priority.

- Providing for entities internal to a Control Area (IPPs, etc..)/Requiring tighter granularity in the scheduling process (source to sink, not just CA to CA) – The issues Task Team

believes that this is an important issue, but wanted more group consensus before identifying it as a top priority.

Should be possible but not required.

- Offering "one-stop shopping" to PSEs – The concept of "one-stop shopping" is ambiguous. Does this refer to the above need to eliminate redundant data entry? An ability to reserve energy and transmission at the same time? An ability to identify a source and sink and have necessary transmission procured?

One stop shopping defined is an ability to provide (thought internal or external development) a method in which one application can be used to schedule. – Barbara wants to talk about it.

- Designing the system to provide for different energy types – what sorts of types are there? Do these need to be standardized? Or will these remain as a part of "regional diversity?"

Needs to be handled in the data model

- Integrating Electronic Scheduling with existing EMS systems – to what degree of integration are we referring? For example, should a PSE be able to submit a schedule directly to an EMS system once confirmed? Is there a "scheduling interface" between the Electronic Scheduling system and the EMS? Do operators only receive "net schedules," and never see individual transactions?

Needs to be in the data model

- Registering and formalizing business rules – Does this mean diversity is acceptable, but variances from pro-forma must be filed at a central information distribution point? Does it mean business logic must be implemented through electronic means so that the user is not required to manage the information as closely?

Probably need to be a top issue

- Keeping operations free from market concerns/keeping the market free from operating concerns – this is a much more complex issue than it appears. Obviously, the market and operations must be linked in some ways due to their very nature. However, how tightly must they be linked? For example, does an operator need to know detailed transaction information so that transactions can be "cut" to relieve congestion? Or should operators be asked to reduce scheduled interchange, and leave the management of the transactions to the security coordinators and the market? Should operators be burdened with knowledge of financial information? Should marketers be required to understand ramping rules and other operational data in order to buy and sell power?

This is important too, but there will be some shared information.

- Providing a centralized solution – there was some confusion as to what a "centralized solution" referred to. For example, does this refer to one scheduling system, developed by NERC, that everyone should use? Or a centralized interface point provided by NERC

that allows access to proprietary scheduling systems, thus insulating the marketer from regional diversity? In order to properly determine the value of this issue, it must be explored further.

Same as one stop shopping

- Allowing the use of multiple transmission rights across time (horizontal stacking) – this refers to the concept of using several time-based blocks of transmission to transact across a longer period of time (for example – Res A from 9-10 am, Res B from 10 –11 am, Transaction runs from 9-11am). This may be more of an implementation detail than an issue, but flexibility in the system for defining usage is an issue that should be further discussed and addressed.

Important

- Permitting custom interfaces to accommodate regional needs – does this refer to *user* interfaces or *machine* interfaces? Or both? A common data standard for machine-to-machine interfaces seems to be a given requirement, but should we examine standardized user interfaces as well?

Important

- Providing for in-kind losses – where is the industry moving with regards to this issue? In some ways, it seems that this is going to disappear in the future through the provision of losses as an Ancillary Service. What are the feelings of the ESTF?

Important

1998 OASIS Phase 2 Survey

In 1998, EPRI commissioned a similar survey. This survey identified many of the same concerns and developed many of the same results. Some notes of interest:

- Transmission Customers wanted to ensure confidentiality of transaction information (note: this did not identify whether "transaction information" referred to price, scheduling/interchange path details, or both, which may account for the seeming change in disclosure philosophy seen in the recent months)
- Transmission Customers wanted to have the option to pay for redispatch as opposed to curtailment when a constraint limits their transaction
- Transmission Customers were neutral on the concept of flow based reservations (as opposed to contract path)
- Transmission Providers and Control Areas felt enhancing performance, reducing processing time, and improving system reliability through the use of automation was an important issue that needed to be addressed
- Independent System Operators and Power Exchanges felt that a NERC-wide scheduling model would not address their specialized needs and requirements

Conclusion

It seems that we have a good foundation of issues to include in our discussions. We have identified several consensus issues, as well as several additional discussion items. Throughout the process, it will be important to continue to keep monitoring consensus in various ways to ensure that the system continues to serve its stakeholders needs properly.

Issues Survey - Sorted by Mean Rating

Question	Responses				
	Mean	***Mode***	***Median***	***Min***	***Max***
Making the system extremely reliable.	9.423	10	10	6	10
Dealing with curtailments.	9.385	10	10	7	10
Requiring reliable networking, telecommunications, and computer hardware.	9.231	10	10	6	10
Improving operations efficiency.	9.154	10	10	5	10
Modifying a schedule after it has begun.	9.154	10	10	5	10
Reducing redundant data entry.	9.120	9	9	5	10
Correctly assigning responsibility to the proper entities.	8.962	10	10	3	10
Providing for the hourly market.	8.885	10	10	5	10
Providing a consistent interface to users.	8.880	9	9	6	10
Providing the best Electronic Scheduling product possible.	8.880	10	9	5	10
Designing to expand/extend functionality easily.	8.880	9	9	6	10
Offering electronic interchange schedule confirmation.	8.800	10	10	5	10
Achieving majority stakeholder acceptance.	8.750	10	9	4	10
Implementing NERC-wide naming conventions.	8.731	10	9	5	10
Incorporating automatic check-out functions.	8.720	10	9	6	10
Incorporating scheduling timeframes (hourly, daily, weekly).	8.600	10	9	1	10
Making a fast process that can be automated extensively.	8.520	8	9	5	10
Keeping systems simple and straightforward.	8.462	10	9	2	10
Integrating OASIS with scheduling.	8.400	10	9	1	10
Streamlining the market interface.	8.320	9	9	6	10
Distribution of information to all counterparties.	8.269	10	9	4	10
Creating NERC-wide scheduling standards.	8.240	10	9	1	10
Providing for entities internal to a control area (IPPs, etc…).	8.240	10	9	1	10
Dealing with loss accounting and ancillary services.	8.160	10	9	5	10
Transitioning in planned, incremental steps.	8.160	8	8	4	10
Scheduling energy and transmission together.	8.000	8	8	3	10
"Raising the bar" to force progress and ensure proper standards.	8.000	8	8	3	10
Allowing for electronic verification of rights transfers for both energy and transmission.	8.000	8	8	1	10
Involving RTOs in the collaborative process.	7.960	9	9	4	10

Having scheduling systems create tags for reliability monitoring.	7.920	10	8	1	10
Offering "one-stop shopping" to PSEs.	7.840	9	8	2	10
Achieving industry consensus.	7.769	8	8	4	10
Designing the system to provide for different energy types.	7.731	9	9	2	10
Implementing common business practices across Interconnections.	7.692	8	8	1	10
Integrating Electronic Scheduling with existing EMS systems.	7.560	10	9	1	10
Registering and formalizing business rules.	7.560	10	8	1	10
Keeping operations free of market concerns.	7.500	10	9	1	10
Providing "hooks" for other legacy and future systems.	7.400	8	8	3	10
Providing a centralized solution.	7.269	10	8	2	10
Mandating an industry-wide training program.	7.269	10	7	1	10
Allowing use of multiple transmission rights across time (horizontal stacking).	7.200	10	8	2	10
Implementing automatic processing of inadvertent, AIE, etc…	7.200	7	8	1	10
Permitting custom interfaces to accommodate regional needs.	7.200	10	7	1	10
Improving the registration process.	6.920	6	7	1	10
Consulting with outside process modeling developers.	6.840	7	7	1	10
Providing for in-kind losses.	6.800	10	7	1	10
NERC-wide addressing congestion management.	6.760	9	8	1	10
Implementing Electronic Scheduling as soon as possible.	6.560	6	7	1	10
Requiring tighter granularity in the scheduling process (source to sink, not just CA to CA).	6.520	10	7	1	10
Providing functionality for use with Retail.	6.000	5	5	1	10
Allowing for regional diversity.	5.960	3	7	1	10
Providing operators with one net schedule instead of multiple transactions.	5.840	5	5	1	10
Implementing flow-based reservations.	5.840	5	6	1	10
Using tags as the front end to the scheduling system.	5.760	5	5	1	10
Maintaining Contract Path methodology.	5.577	8	7	1	10
Allowing multiple sources and/or sinks on one transaction.	5.520	8	6	1	10
Keeping the market free from operating concerns.	5.280	9	6	1	9
Allowing PSEs to schedule without knowing the complete path (i.e., parking and hubbing).	5.200	5	5	1	10
Implementing based on the "lowest common denominator" to ensure ease of implementation.	5.200	5	5	1	10
Moving away from the Internet in favor of private networks.	5.154	5	5	1	10
Standardizing of tariffs.	5.000	5	5	1	10
Eliminating tagging and OASIS and starting over.	5.000	1	5	1	10
Buying/Selling energy on an OASIS like system.	4.960	1	5	1	10
Tracking financial information as well as operational.	4.520	1	5	1	9
Providing an interim solution until we develop a permanent solution.	4.360	5	5	1	10

Processing non-physical transactions.	4.240	1	3	1	10
Maintaining PSE to PSE Confidentiality.	3.792	1	4	1	10

Issues Survey - Sorted by Mode Rating

Question	Responses				
	Mean	***Mode***	***Median***	***Min***	***Max***
Making the system extremely reliable.	9.423	10	10	6	10
Dealing with curtailments.	9.385	10	10	7	10
Requiring reliable networking, telecommunications, and computer hardware.	9.231	10	10	6	10
Improving operations efficiency.	9.154	10	10	5	10
Modifying a schedule after it has begun.	9.154	10	10	5	10
Correctly assigning responsibility to the proper entities.	8.962	10	10	3	10
Providing for the hourly market.	8.885	10	10	5	10
Providing the best Electronic Scheduling product possible.	8.880	10	9	5	10
Offering electronic interchange schedule confirmation.	8.800	10	10	5	10
Achieving majority stakeholder acceptance.	8.750	10	9	4	10
Implementing NERC-wide naming conventions.	8.731	10	9	5	10
Incorporating automatic check-out functions.	8.720	10	9	6	10
Incorporating scheduling timeframes (hourly, daily, weekly).	8.600	10	9	1	10
Keeping systems simple and straightforward.	8.462	10	9	2	10
Integrating OASIS with scheduling.	8.400	10	9	1	10
Distribution of information to all counterparties.	8.269	10	9	4	10
Creating NERC-wide scheduling standards.	8.240	10	9	1	10
Providing for entities internal to a control area (IPPs, etc…).	8.240	10	9	1	10
Dealing with loss accounting and ancillary services.	8.160	10	9	5	10
Having scheduling systems create tags for reliability monitoring.	7.920	10	8	1	10
Integrating Electronic Scheduling with existing EMS systems.	7.560	10	9	1	10
Registering and formalizing business rules.	7.560	10	8	1	10
Keeping operations free of market concerns.	7.500	10	9	1	10
Providing a centralized solution.	7.269	10	8	2	10
Mandating an industry-wide training program.	7.269	10	7	1	10
Allowing use of multiple transmission rights across time (horizontal stacking).	7.200	10	8	2	10
Permitting custom interfaces to accommodate regional needs.	7.200	10	7	1	10
Providing for in-kind losses.	6.800	10	7	1	10
Requiring tighter granularity in the scheduling process (source to sink, not just CA to CA).	6.520	10	7	1	10
Reducing redundant data entry.	9.120	9	9	5	10
Providing a consistent interface to users.	8.880	9	9	6	10

Designing to expand/extend functionality easily.	8.880	9	9	6	10
Streamlining the market interface.	8.320	9	9	6	10
Involving RTOs in the collaborative process.	7.960	9	9	4	10
Offering "one-stop shopping" to PSEs.	7.840	9	8	2	10
Designing the system to provide for different energy types.	7.731	9	9	2	10
NERC-wide addressing congestion management.	6.760	9	8	1	10
Keeping the market free from operating concerns.	5.280	9	6	1	9
Making a fast process that can be automated extensively.	8.520	8	9	5	10
Transitioning in planned, incremental steps.	8.160	8	8	4	10
Scheduling energy and transmission together.	8.000	8	8	3	10
"Raising the bar" to force progress and ensure proper standards.	8.000	8	8	3	10
Allowing for electronic verification of rights transfers for both energy and transmission.	8.000	8	8	1	10
Achieving industry consensus.	7.769	8	8	4	10
Implementing common business practices across Interconnections.	7.692	8	8	1	10
Providing "hooks" for other legacy and future systems.	7.400	8	8	3	10
Maintaining Contract Path methodology.	5.577	8	7	1	10
Allowing multiple sources and/or sinks on one transaction.	5.520	8	6	1	10
Implementing automatic processing of inadvertent, AIE, etc…	7.200	7	8	1	10
Consulting with outside process modeling developers.	6.840	7	7	1	10
Improving the registration process.	6.920	6	7	1	10
Implementing Electronic Scheduling as soon as possible.	6.560	6	7	1	10
Providing functionality for use with Retail.	6.000	5	5	1	10
Providing operators with one net schedule instead of multiple transactions.	5.840	5	5	1	10
Implementing flow-based reservations.	5.840	5	6	1	10
Using tags as the front end to the scheduling system.	5.760	5	5	1	10
Allowing PSEs to schedule without knowing the complete path (i.e., parking and hubbing).	5.200	5	5	1	10
Implementing based on the "lowest common denominator" to ensure ease of implementation.	5.200	5	5	1	10
Moving away from the Internet in favor of private networks.	5.154	5	5	1	10
Standardizing of tariffs.	5.000	5	5	1	10
Providing an interim solution until we develop a permanent solution.	4.360	5	5	1	10
Allowing for regional diversity.	5.960	3	7	1	10
Eliminating tagging and OASIS and starting over.	5.000	1	5	1	10
Buying/Selling energy on an OASIS like system.	4.960	1	5	1	10
Tracking financial information as well as operational.	4.520	1	5	1	9
Processing non-physical transactions.	4.240	1	3	1	10
Maintaining PSE to PSE Confidentiality.	3.792	1	4	1	10

Attachment 5

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Electronic Scheduling Collaborative/ NERC Electronic Scheduling Task Force

Electronic Scheduling Collaborative Business Practices Survey Summary

January 25, 2001

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Electronic Scheduling Collaborative
Business Practice Survey Results

Introduction and Overview

In response to FERC issuing its ANOPR on OASIS Phase II, the ESTF formed an Electronic Scheduling Collaborative (ESC) to encourage more participation by all industry segments in the NERC Electronic Scheduling effort.

The work of the ESC was divided into two phases. In Phase I the ESC will work toward an industry consensus filing in response to the FERC ANOPR. Phase II will continue the work of the ESTF in completing all aspects of the transmission and energy scheduling process.

FERC's ANOPR presented several challenges to the ESC. One of the tasks identified was the need to understand the current Transmission and Interchange Scheduling practices in the industry. The ESC decided to issue a survey to gain an understanding of the various market participants' business practices that currently exist. This information will be useful in determining the functional requirements for electronic scheduling in response to FERC's ANOPR.

The objectives of the survey were:

1. Compare information needs among the different market participants e.g. what information is needed, when schedules must be submitted, time to complete an electronic schedule, and so on, and
2. Identify necessary interfaces to other systems (existing and new) in order to meet performance requirements.

The survey questions were divided into seven areas of responsibility, which are listed below:

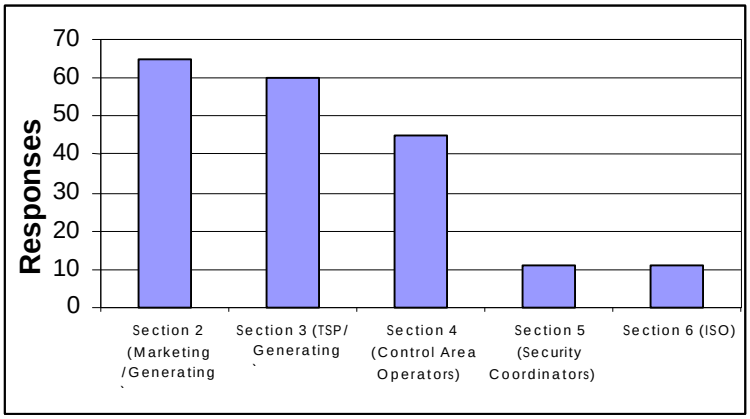
1. Tell Us About Yourself. (Name, Organization, ISO/CA affiliation, NERC region, etc.)
2. Marketing Entity
3. Transmission provider
4. Generating Entity
5. Control Area
6. Security Coordinator
7. ISO / RTO

The first section "Tell Us About Yourself" was used to establish the background and affiliation of the respondent.

Electronic Scheduling Collaborative
Business Practice Survey Results

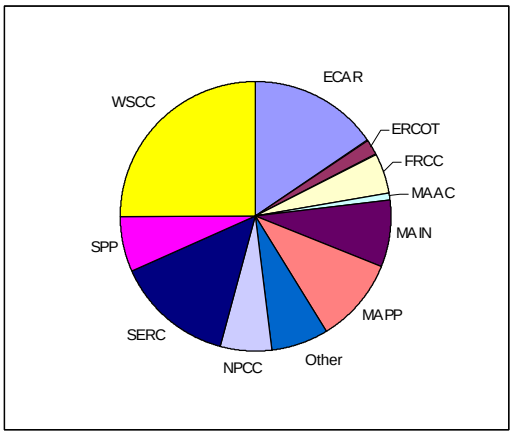
Result Summary

There were 192 entities that responded to the survey representing different regions and perspectives from the industry. Responses to the survey sections are shown in the chart to the right.



The following NERC Regions supplied responses in the summary. The pie graph shows the overall percentage responded by Region.

- **ECAR**
- **ERCOT**
- **FRCC**
- **MAAC**
- **MAIN**
- **MAPP**
- **OTHER**
- **NPCC**
- **SERC**
- **SPP**
- **WSCC**



An average score has been placed on some of the survey questions. For questions that asked the respondent to place a ranking between 1 and 6, 1 being "Strongly Agree" and 6 being "Strongly Disagree" the following example shows how the simple average was calculated on the survey.

	Votes	Weighted Score
1. Strongly Agree	25	1x25 = 25
2.	16	2x16 = 32
3.	4	3x4 = 12
4.	3	4x3 = 12
5.	3	5x3 = 15
6. Strongly Disagree	1	6x1 = 6
Total	59	144

The average score for the results of this example question would be (144/59), or 2.4407, which would reflect a preference towards Agreeing.

The results of the survey illustrate the disparity of business practices throughout the industry. Very few questions had a high consensus by the respondents.

A copy of the Business Practice survey and results can be found at http://www.nerc.com/~filez/eScheduling.html.

Comment Summary

The survey also requested respondents to submit comments. A summary of these comments follows:

Section 2c (Marketing/Generating Entities)

Question 11 – *What information do you supply, beyond that being collected for Etag, to satisfy scheduling requirements?*

Six "none"
Three Energy product type
Four Specific requirements by Control Area
Five Scheduling ID, Energy ID, contract number, schedule type or scheduling agent
Two Price
One Sink price cap
One Source unit
One Ramp
One interruptible level

Question 12 – *Additional comments regarding Electronic Scheduling?*

Six thought it needed to be kept simple, less cumbersome to use and reduce the costs of a complex system.
Four thought uniformity/common format was important
Two recommended using a single time zone
Two didn't think electronic scheduling was required, Etag was the schedule.
One wanted to make sure a denied tag could be updated and resubmitted
One thought the market (not NERC) should drive the development of an electronic scheduling system.
One wanted to make sure there was sufficient training period between the completion of the application and its implementation.

Question 13 – *Are there any other business practice issues or comments that you feel need to be addressed?*

Five wanted there to be more consistency throughout the regions.
Remaining comments could not be grouped

Section 3 (Transmission Service Provider/Generating Entity)

Question 14 – *What other reasons would you deny a tag besides what is listed above?*

Six responded with "Late" or "timing requirements"
Two had invalid MW and OASIS combination
Remaining comments could not be grouped

Question 24 – *What information do you need, beyond that being collected for Etag, to satisfy your needs?*

Six Responses were approval and confirmation related.
Four wanting active approval
One wanting PSE's to have approval rights.
One wanting the transmission provider rights to confirm energy source.
Two wanted details on schedule type.
Remaining comments could not be grouped

Question 25 – *Additional comments regarding Electronic Scheduling?*

Two responses wanted positive/mandatory confirmation of schedules.
Remaining comments could not be grouped

Question 27 – *Are there any other business practice issues or comments that you feel needs to be addressed?*

Two responses said they already use Etags as schedules
Two responses wanted dynamic scheduling to be addressed
Two responses wanted to ensure source and sink information is provided
Two wanted to express concerns about moving forward with parking and hubbing.
Remaining comments could not be grouped

Section 4 (Control Area Operators)

Question 27 – *What information do you need, beyond that being collected for E-tag, to satisfy your scheduling requirements?*

Five responses said correct Etags are has sufficient information
Two thought it might be useful to have the energy type (i.e. firm, nonfirm).
Two thought specific generating resources could be required.
Two wanted to ensure source/sink information is provided.
Remaining comments could not be grouped

Question 15 – *Additional comments regarding electronic scheduling?*

This section had many good comments that stand on their own and cannot easily be grouped.

Question 16 – *Are there any other business practice issues or comments that you feel needs to be addressed?*

Several comments were issued about the timing of the systems. It needs to be faster and submission of data has to be within the timing requirements.
Remaining comments could not be grouped.

Section 5 (Security Coordinators)

Question 2 – *What information do you need, beyond that being collected for E-tag, to satisfy your scheduling requirements?*

Two wanted to make sure source and sink are required and valid.
Two wanted generation information
Remaining comments could not be grouped.

Question 3 – *What other business practice issues do you feel needs to be addressed? (Comments below)*

Can we identify all tags on an interface by priority?

Need source to sink information for transactions and electronic confirmation from source to sink ASAP. Should consider delaying implementation of proposed fragmented scheduling if it will potentially delay OASIS Phase II.

NERC must be cautious to thoroughly test any scheduling software FULLY in the environment in which it must operate.

Also, NERC should not be setting business practices for transmission providers - these are not reliability issues.

Operators who deal with schedules on a continuing basis would like to see emphasis put on automated error checking

The current E-tag and OASIS is a good foundation on which to build e-scheduling. E-scheduling should evolve – current scheduling systems that use E-tags and OASIS as input must not be made obsolete.

The move to electronic scheduling will be a major step for the industry. Implementation of this step must be timed to avoid the peak summer season. This means the system must be ready to go before April 1 of the year established for implementation.

Question 3 – *Please provide any additional comments you may have regarding electronic scheduling? (Comments below)*

Contract path scheduling. NERC needs to support strongly efforts to develop and implement flow based scheduling methods. This would reduce need for TLR.

Do we need approval of schedule by each transaction participant?
Do we need approval with source and sink vs. only with adjacent SC?

Hubbing/Parking. Need to be able to see the OASIS # without opening the tag

Parking and Hubbing and the resultant masking of ultimate sources and sinks for transactions are a serious threat to the SCs being able to perform adequate and meaningful security analysis.

Scheduling deadline for firm should be clearly set as noon the day before (with no exceptions for "Firm") and NERC should set a standard (and measure it) of entering the next day in a secure state (at least on a Firm basis with no new contingencies).

The majority of the Eastern Interconnection transmission providers now use E-Tag as the schedule or the source of the scheduling information. Planned E-Tag 1.7 enhancements will make it even easier to use E-tag as the schedule.

Transmission Reservations – need to address the use of electronic schedules as substitutes for current way of making reservations for short-term transmission reservations. Security Assessment-how to ensure only full path E-Tags, not partial path E-Tags

Business Practice Analysis

A paper illuminating the common business issues has been created. This paper takes the first steps in separating current industry issues into potential business practices and other items to be considered while creating new business practices for the industry.

Conclusion

The business practice group has summarized the existing business practices and plans on working with other NERC committees and industry participants to produce a set of common business practices for industry that can be used in support of OASIS Phase II.

Attachment 6

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

OASIS Phase II
Business Practices Development Summary

A Representative List of
Business Practice Issues

For

OASIS Phase II

February 2001

I. Introduction

The Industry needs to have game plan for the on-going development of OASIS Phase II Business Practices. A set of practices must be identified that can be as uniform and standard as possible throughout North America. ESC has identified two classes of business practices, those that will be filed to ensure that open and competitive markets are accommodated in a consistent manner, and those that may not necessarily be filed, but are necessary to accommodate regional differences in both reliability and markets.

The ESC also feels that any Business Practices identified to be filed with the FERC will require more than just the ESC Business Practices Task Groups involvement. Each Business Practice to be filed needs to have a list of Stakeholders, and a single identified working body that would be responsible for the development of the filed Business Practice. A partial list of Stakeholders would include: PSEs, Generators, Security Coordinators, RTOs, NERC Regional Compliance offices, Marketers, Control Areas/Balancing Authorities, Scheduling Authorities, etc. A partial list of the groups that must collaborate in the development of a given Business Practice would include:

- Market Interface Committee (MIC)
- MIC's Market Interface Practices Subcommittee (MIPS)
- MIC's Congestion Management Subcommittee (CMS)
- MIC's Next-Hour Market Subcommittee (NHMS)
- Operating Committee (OC)
- OC's Interchange Subcommittee (IS)
- Electronic Scheduling Collaborative (ESC) / Electronic Scheduling Task Force (ESTF)
- OASIS Standards Collaborative (OSC) / Transaction Information System Working Group (TISWG)
- ESC's Business Practices Task Group (ESCBPTG)
- OSC's Business Practices Task Group (OSCBPTG)
- ESC Losses Task Group (ESCLTG)
- Control Area Criteria Task Force (CACTF)
- Interchange Distribution Calculator Working Group (IDCWG)
- RTO Seams Groups
- Regional MIC groups

Others interested in participating in the development of Business Practices are invited to participate in the open ESC effort.

It is important to distinguish between Market Practices and Scheduling Practices. We also need to keep in mind the items that will impact current NERC Policy. Also, the reverse is true, we need to keep in mind that we are asking that the FERC approve the Business Practices and therefore administer the Business Practices. The other Practices that are not filed may still require the modification or addition to the existing NERC Policies.

Our short-term goal is to develop Business Practices necessary to support the implementation of OASIS Phase II as required by the FERC. We need to evaluate Business Practices as to whether they will stand the test of time for OASIS Phase II.

The ESC recognizes that the industry is experiencing many changes, including the new Control Area Criteria Task Force Reliability Model, and the NERC/NAERO Transition/Legislation. The emerging seams and the elimination of seams due to formation of RTOs will be a constantly moving target. The fact that the FERC

has approved a variety of RTO Market Models is a complicating factor. Not all RTOs will be operational on December 15, 2001. The number of non-jurisdictional entities that may or may not join RTOs in the short-term is an issue. Marketing entities will still have to deal with a variety of scheduling practices because not all entities will be a part of an operational RTO and all business practices may not be standardized. The fact remains that the timing of the implementation of OASIS Phase II will be complicated by the ever-changing landscape of the industry.

II. Major Business Practices that may be filed with FERC

A. **Schedule Timing (Filed BP)** — Provide a minimum timing standard for submitting and responding to resource and schedule requests. This is a critical issue that the ESC must resolve for Oasis Phase II and for action by FERC. A "Timing Group" has been formed to address these timing issues.

B. **Scheduling process including Modifications/Adjustments** — Need to identify the different schedule modifications that can be made, by which function the modifications are handled, and who can make the change and when.

C. **Ramping Rules** — Define rules for duration and start times for ramping transactions.

D. **Schedule Implementation Time, Granularity** — Define rules for when schedules can start and stop.

E. **Standard Terminology** — A dictionary will be filed with FERC filing for Business Practices.

F. **Losses** — Determine the methods for loss compensation.

G. **Approval Process** — Who has rights to approve reservations and schedules, and whether those approvals are active or passive.

H. **OASIS Phase II Registration Requirements** — Define items subject to registration processes for business entities, resources, services, etc.

III. Business Practices that impact the OSC and the S&CP Development, which may or may not be filed with FERC

A. **Schedule Composition** — Define what data details constitute a schedule.

B. **Congestion Management** — ESC will try to accommodate all FERC approved RTO congestion management concepts.

C. **Dynamic Schedules for Network Service, Joint Owned Units, and Other Types of Schedules** — Identify all types of schedules and what considerations need to evaluated.

D. **Facilitate Markets** — Facilitate markets with necessary data e.g. pricing data, auction bidding, etc.

E. **Backup Communications** — Define business rules to support OASIS Phase II during communications failures.

F. Dealing with Non-RTO/non-jurisdictional Entities

G. **Scheduling of Ancillary Services** — Identify if Business practices are needed.

H. **Settlements** — Identify if Business practices are needed.

I. **Security Requirements** — Determine what data needs to be secured, at what level and using what technology.

J. **Transmission Status Posting** — Identify what transmission data (i.e. flows and limits on critical flowgates) needs to be posted on OASIS Phase II.

K. **Controllable Devices** — Define business practices for Phase-Shifting Transformers and DC facilities.

L. **Secondary Transmission Market** — Determine what business practices, if any, need to be defined for secondary markets.

M. **Graphical User Interface (GUI) Standard Templates** — Identify navigation paradigms for user displays.

N. **Stacking of Transmission Rights** — Determine business practices associated with using multiple transmission reservations to support a single transaction.

Attachment 7

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Electronic Scheduling Collaborative/ NERC Electronic Scheduling Task Force

Electronic Scheduling Collaborative Generator-Run Status Position Papers

January 25, 2001

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Generator-Run Status:
Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II

January 29, 2001

1. Summary

This paper is written in support of broad disclosure of system information to the market, including information regarding the status and loading of generating units connected to the major electrical interconnections in the United States. Generator run status is a critical element of information used by many entities to ensure the operating security of the interconnected electric system. It should also be a component of the information base made available to all participants in the bulk power market to ensure appropriate market responses to real-time operating conditions, to provide the transparency needed for economically efficient markets, and to add discipline and market power mitigation through analysis of data to reveal patterns of strategic behavior.

Each of us would like to go about the business of generating, buying, selling and delivering energy to our customers acting like our own actions – our business decisions – affect us and our own customers alone. But the fundamental facts are exactly the opposite. Industry stakeholders, NERC, FERC and the states are consumed by the unintended, unmitigated effects of interconnected operations in an industry now characterized by a highly congested grid, tight generating capacity margins and untested rules for market operation. The old rules for market participant behavior no longer work. The new ones are still being written.

To summarize the views of the proponents of generator run status disclosure:

- We do not seek disclosure on OASIS of any marketer's trading book or contract portfolio.
- We do not seek the uniform disclosure of ***forecasts*** of generator run status data, although the posting of such information may be required in other contexts such as for RTO reliability must-run units.
- We do seek a level playing field through access to real-time operating information now provided to many operating authorities. This information includes:
    1. the status of breakers (open/closed),
    2. generating unit MW and MVAR capability,
    3. MW and MVAR net output and
    4. status of automatic voltage control facilities.
- We advocate disclosure on OASIS, as close to real-time as is feasible, sufficient information for third parties to understand and respond rapidly to the physical effects of regional generator operating conditions (including dispatch levels and outages). Changes in generator run status may affect third parties through curtailments due to reduced transfer capability, as well as changes in relative prices that affect decisions to buy or sell energy on the spot market. Some masking or aggregation of unit-specific data may be appropriate to balance commercial and public policy interests.

- After the fact, we seek more comprehensive disclosure of unit-specific data on generator output and operating status, to permit market participants to perform audits of the market behavior of other entities who's actions may adversely affect our operations. A short lag (e.g., one day after close of the trading period) may be appropriate to allow time for error correction and to balance commercial and policy interests.
- We do not view the posting of other data (such as the net flows over commercially significant flowgates) as a good substitute for generation run status data.

2. Background

In Docket No. RM00-10-000 (the OASIS ANOPR) the Commission set in motion efforts to create the second, planned phase of OASIS implementation. In the ANOPR, FERC states that "the industry should consider whether generator-run status information should be incorporated into OASIS Phase II." This issue has been raised previously under FERC Order 605 (Docket No. RM98-3-000), issued May 27, 1999, where FERC extended the retention period and availability of information on curtailments and interruptions. Order 605 modifies Order 889 to require the posting of "information to support any such curtailment or interruption, including the operating status of the facilities involved in the constraint or interruption." In our view, such information can and should include the status of both transmission and generation facilities.

Information disclosure and posting does not take place in isolation from other developments. Indeed, the electric power industry has been characterized by the following statements and allegations: "market dysfunction"[1], "violations of standards of conduct"[2], failure to provide timely notification of curtailments[3], "inability to obtain critical information concerning general problems, such as the *causes of* TLRs"[4], an "environment ripe for collusion"[5], and "chronic pattern of underscheduling"[6]. Yet in most instances cited, investigators have been unable to obtain sufficiently detailed information through public posting and voluntary disclosure, to even decode what has happened, much less to pursue legal action and seek contractual remedies for non-performance.

The industry must now decide whether rules for information disclosure to security authorities and to bulk power market participants should be characterized by information transparency, or policies that create pools of proprietary information that may favor certain market participants. From the perspective of the authors, disclosure of generator run status is not a black and white issue. Rather, the concerns and needs that must be addressed and weighed reflect many of the complex reliability, regulatory and commercial policy issues raised by electric restructuring. We

---

1 FERC, "Market Order Proposing Remedies For California Wholesale Electric System". Docket No. EL00-95-000, et al. November 1, 2000. Numerous citations.

2 FERC, "Staff Investigation of Bulk Power Markets: Southeast Region". November 1, 2000. Page 3-42.

3 FERC, "Staff Investigation of Bulk Power Markets: Northeast Region". November 1, 2000. Page 1-72.

4 FERC, "Staff Investigation of Bulk Power Markets: Midwest Region". November 1, 2000. Page 2-31.

5 Restructuring Today. October 27, 2000. Quote by Robert McCullough regarding conditions in the California power market.

6 FERC, "Market Order Proposing Remedies For California Wholesale Electric System," Docket No. EL00-95-000, et al. November 1, 2000. Page 23.

recognize that market participants have legitimate commercial interests to protect and these interests may be adversely affected by the disclosure of some of the data elements discussed below. However, our recommendations are also predicated on the following additional facts and considerations:

- Competitive, liquid markets require a level of information transparency that is lacking in most bulk power markets in North America.
- Much of the time, bulk power markets do not behave like a textbook competitive market. If the market were truly competitive, the outage of a single unit would not expose the owner to price discrimination when it seeks to replace a lost generating unit.
- Other purchasers and sellers in the region, not just the unit owner, are adversely affected by generating unit outages, through increases in the spot market price for replacement energy and through curtailment of interchange transactions due to decreased transfer capability (increased congestion and loop flows).
- Many wholesale and retail merchants already have preferential access to the information for which we seek disclosure, due to the other functional hats they wear (as transmission providers and control areas) or due to the dominant positions that many vertically integrated utilities now have in regional generation markets.
- Wholesale generation markets have not been "deregulated." Rather, authorization for a specific seller to charge market-based rates in a particular market is conditioned on whatever reporting and disclosure requirements FERC may impose.
- Most transmission, control area and interconnected operation services are not now provided and will not be provided by large, independent, fully functional and effective Regional Transmission Organizations for at least two to five years. Indeed, FERC has *not* mandated RTO participation.
- Market monitoring by RTOs and FERC is not an adequate substitute for providing market participants with sufficient information to understand the conduct of other market participants.
- Even if monitoring were a viable alternative to data disclosure, most wholesale transactions are unlikely to be monitored closely. Order No. 2000 does not require RTOs to monitor the entire bulk power market. Rather, each RTO Market Monitoring Unit (MMU) is charged with monitoring the generation and transmission markets operated by the host RTO. FERC staff lacks the resources, data and policy directives to monitor the bulk power market in any significant detail except during crisis conditions (as in California). Bilateral transactions (and the power flows that result from such transactions) are not today monitored by any non-security authority. Internal economic dispatch to serve native load is also insulated from market monitoring.

3. Description of Generator-Run Status Information

A. Actual Generator Telemetry Data

The Commission did not elaborate on the term "generator-run status" in the ANOPR or Order 605. For purposes of this paper, the term refers to the following current and historical

information regarding each generating unit of any powerplant that is interconnected to the bulk power system:[7]

1. Status of breakers (open/closed)
2. Unit MW and MVAR capability
3. MW and MVAR net output
4. Status of automatic voltage control facilities

The most critical information requirements are the public postings of actual plant performance data on a current and after-the-fact basis. For purposes of NERC compliance, control area operators poll this information at least every ten minutes. It is feasible to reproduce this information on a secure gateway to an OASIS site or other Internet server accessible by market participants and interested parties.

B. Forecast Generator Information

While a strong case can be made that this information should be disclosed and posted for forecast periods, the authors concluded that disclosure of forecast data raises greater commercial/market sensitivity concerns than real-time and historical data. In addition, forecasts can be unreliable and may themselves be manipulated for strategic reasons.

For purposes of predictive security assessment and ATC calculations, we expect that forecast information will still be provided to the relevant organizations. These organizations will also have access to actual performance data and should be encouraged to scrutinize any attempt to misrepresent the cause of outages, deratings or other actions that affect reliability or transmission transfer capabilities.

4. Pretense of Fully Competitive Generation Markets

While it is FERC's objective to create competitive generation markets by eliminating market power and monopolies, recent experience suggests that attaining this goal cannot be simply assumed by the mitigation of vertical market power through open-access transmission.[8] FERC Order 2000 is based on the Commission's conclusion that *perceptions* of discriminatory and preferential treatment, and other market structure problems must be eliminated. Horizontal market power in generation continues to affect purchasers that have limited supply options when transmission constraints are present. Thus it is false to presume the existence of full and fair competition that is sufficient to provide consumer benefits in most power markets.

In spite of the high ethical standards prevalent in our industry, if information is withheld, information leaks will occur. Those who have access to leaked information will profit at the expense of those playing by the rules. There is a clear need for reliable, current information by all operating and merchant segments of the electric industry. The industry will save itself a considerable amount of difficulty ensuring fair treatment of all industry segments by adopting a simple, straightforward process of disclosure.

---

[7] A size threshold is appropriate here, but may vary regionally.

[8] Bushnell, James, Christopher Knittel and Frank Wolak. Estimating the Opportunities for Market Power in a Deregulated Wisconsin Electricity Market. November 2000. Tabors Caramanis and Associates. Horizontal Market Power in Wisconsin Electricity Markets. November 2, 2000.

While disclosure of generator run status may affect the competitive position of some market participants, a broader public policy goal of ensuring elimination of market power[9] prior to releasing the forces of market competition must first be implemented. To claim that generator status disclosure is anti-competitive is not correct when circumstances dictate that full and fair competition cannot exist given the presence of market power. Disclosure of generator run status information provides essential information to directly measure the exercise of horizontal market power.

5. Past Precedent on Proprietary Information and Confidentiality

Opponents of generator run status disclosure appear to take the position that information about their generating facilities is private property that they cannot be compelled to disclose. Disclosure is compared with "confiscation of private property." Considering the breadth of current government and self-regulating organization disclosure rules in almost every other segment of the U.S. economy, this is a gross over-exaggeration. Specifically, FERC prescribes certain mandatory reporting requirements for Electric Utilities using its statutory authority under the Federal Power Act.[10]

The Energy Information Administration (EIA) of the Department of Energy (DOE) is required to publish, and otherwise make available to the public statistical data that reflect national electric supply and demand activity as accurately as possible. To meet this obligation, as well as internal DOE requirements for accurate data, the Electric Power Division of the EIA has developed statistical surveys that encompass each significant electric supply and demand activity in the United States.[11] In processing a Freedom of Information Act request the Energy Information Administration wrote:

> "The question of whether substantial competitive harm will in fact occur (by release of data to the public) is a highly fact-specific one. The harm must be substantial, a mere negative effect alone does not meet the standard of substantial harm. Actual competition is a prerequisite if seeking exception from disclosure under FOIA. The entity must be operating in a competitive market, not a non-competitive market. Blanket allegations of harm will not suffice as proof of substantial harm. The burden is on the entity seeking confidential treatment of data. When granting an exemption under FOIA, the question of balance between public interest and the rights of the submitter are always at issue."
>
> *Federal Register, Vol. 63, No. 137, p. 38621 (Published Friday, July 17, 1998)*

In this instance the Commission will be asked here to make a public interest determination. There are numerous other instances where the Commission has found that open disclosure of

---

9 Market power is defined as the ability of a seller to maintain prices above competitive levels for a significant period of time.

10 16 USC Sec. 825c, 16 USC Sec. 825h, 16 USC Sec. 825j. See the FERC web page for a listing of current reporting requirements and list of reports: http://www.ferc.fed.us/electric/electrc2.htm. "Electric Utility" means any person or State agency (including any municipality) which sells electric energy; such term includes the Tennessee Valley Authority, but does not include any Federal power marketing agency (16 USC Sec. 796 (22)).

11 See http://www.eia.doe.gov/cneaf/electricity/forms/sselecpower98.html

information claimed to be confidential was necessary in order to perform its duty, imposed by statute, to ensure that customers' rates are just and reasonable. The Commission has also depended on customers looking out for their own best interests in the first instance—bringing complaints, often based on data that is publicly available.[12] This request is not unusual in either the electric or gas industry, and similar past precedents have not been found to be legally unfair or an act of confiscation.

The public interest criterion has been invoked in other industries where there was disclosure of potential trade secrets. (*Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984)*) Monsanto requested confidentiality on insecticide information submitted to EPA. There was no dispute that the information included trade secrets and that disclosure could cause competitive harm. The Supreme Court ruled that because of the public concern, Monsanto should have known that the data might not remain confidential.

> "As long as [Monsanto] is aware of the conditions under which the data are submitted, and the conditions are rationally related to a legitimate Government interest, a voluntary submission of data in exchange for the economic advantages of a registration can hardly be called a taking." (Registration was "voluntary" in that Monsanto didn't have to register unless it wanted to sell its products in the U.S.)

Similarly, marketers and merchant generators can be given a choice when registering for Exempt Wholesale Generator status if they intend to sell their products in the U.S.

6. Purposes of Generator-Run Status Information

A. System Security Assessment

In the wake of restructuring, FERC open-access, system disturbances and technological advances, the NERC governing board embarked on a series of Security Initiatives in the mid-1990s. A critical element of the NERC Security Initiatives has been the establishment of the NERC Security Processes, including the implementation of the Interregional Security Network (ISN), creation of regional Security Coordinators, and development of policies to support interconnection-wide security assessment. Operating Policy 4.B. provides that certain Operational Security Information will be exchanged among Control Area Operators and Security Coordinators, but will not be disclosed to Purchasing-Selling Entities. Generator-Run Status information is a subset of the Operational Security Information.

It is not disputed that this information is critical to the NERC Security Processes. There are however, concerns about the implications of the "Confidentiality Agreement for Electric System Security Data" that currently limits the availability of this data to control area entities and security coordinators. It has been alleged that some control area entities that have the ability to exercise market power are not able to meet all standards for FERC open-access. In particular, FERC's recent Staff Investigations of Bulk Power Markets reveal that standards of conduct are not adequately monitored, OASIS requirements to provide timely information on system conditions and curtailments are often ignored, and that in general information needed by the market is lacking.

---

[12] Supporting Statement to FERC's Paperwork Reduction Act submission (OMB Control Number 1902-0021) to the Office of Management and Budget, page 6, (July 7, 1998).

When the NERC Operating Committee was considering Policy 4, there was not unanimous support for limiting disclosure of Operational Security Information. A strong minority view was expressed that disclosure of this information would enhance reliability by creating another important feedback mechanism between system conditions and market activity. Such feedback mechanisms are woefully lacking today and the market has been observed to respond in a variety of ways that impair reliable system operations.[13]

B. Benefits for Reliability

Just as electric system operators have found current weather to be an important factor in plant operating strategies, current system conditions are an important element of a reliable operating strategy. In one experience, a merchant in the Midwest noticed that its generator was rotating at a speed equal to a system frequency of 62.5 Hz. CRT displays were going blank, and the generator operator felt that his machine (a small coal fired plant) was at risk. When he inquired to neighboring plant operators about the situation, he was told that there was not a problem on the system. While all of the plants in the area were trying to keep on schedule, the transmission operator failed to notify these merchants that breaker actions had created an island in the system with many hundreds of MW generation in excess of load. These merchants were flying in the dark with only the crude instruments in each of their plants to rely on.

Disclosure and access to more detailed system information, including generator run status for neighboring units, would have prevented this situation from continuing unresolved for a few hours.

Generator status and output can directly affect transmission transfer capabilities. Many path rating nomograms in the Western interconnection demonstrate this property.[14] Capacity Benefit Margins (CBM), used in Available Transmission Capability (ATC) calculations, are based on the run status of certain generating units. Any marketer/merchant that assesses its real-time trading position solely on contracts, synthetic information (ATC postings, market clearing prices, etc.), or hearsay, is going to have difficulty providing reliable power delivery. Again, this situation is likened to flying at night without adequate information and instruments. If you cannot see, and don't have a picture of the environment, only by virtue of hope and prayer will you fly and land safely.

C. Market Discipline

On more than one occasion, FERC has reminded the industry that "information transparency is necessary for a market to function efficiently."[15] Openly available, accurate information disciplines markets and favors no single competitor.

In most commodity markets, relevant information about the status of key production facilities, production and inventory levels, market prices of raw materials, and transportation infrastructure

---

[13] For example, underscheduling and withholding generating capacity in California.

[14] For example, Puget Sound Energy and Seattle City Light generation levels for service to native load directly affect the Northern Intertie Nomograms used to determine transfer limits between Ingledow and Custer. For examples, see http://www.transmission.bpa.gov/OASIS/BPAT/ under the heading Outage Coordination.

[15] FERC, "Staff Investigation of Bulk Power Markets: Midwest Region". November 1, 2000. Page 2-40.

are published periodically.[16] And these are generally commodities that can be stored for periods and in quantities that are orders of magnitude greater than for electricity. Consider metals, petroleum products, and agricultural products—all commodities that trade through open, competitive markets. Bulk inventories in most other commodities are known and provided to the market on-line. The current statistical information provided to these markets is an essential element necessary for rational market response and discipline against market abuse. In this respect bulk power, as a commodity, is no different.

However, from a time perspective, bulk power inventories are measured by generator availability and fuel/water supply. Fuel inventories are known through other commodity markets. Water flows are known in near real-time through a number of public sources.[17] Generators are not like gas wellheads or farmer combines. They convert fuel or falling water into electrical energy. The stability of the transmission system depends on the availability of rotating machinery at every instant in time. It is a serious mistake to compare storable commodities with generator availability.

In this context, information showing correlations between output levels and prices suggests the potential for collusive behavior in California markets. The sources of information for these studies include the WSCC EHV Data Pool, EIA, FERC and EPA databases.[18] Ironically the CAISO has now threatened to withhold EHV data from WSCC, claiming that disclosing "highly market sensitive" information causes "the exercise of market power and gaming in the real time market" and "creates risks to system reliability."[19] What CAISO failed to recognize is that the market and its otherwise informed participants were able to respond to the Power Exchange price signals without discipline. The market rules provided an easy opportunity to ride the price curve by withholding capacity from the system operator until real-time operating emergencies occurred. To make matters worse, power purchasers and public officials were not permitted to analyze real-time information (e.g. EHV Data Pool statistics) that clearly illustrated how the game was being played. That the CAISO market was characterized by certain operating entities taking short positions that led to operating problems should not suggest that the rational solution is to hide the problem from the market. In fact, greater transparency would have enhanced market performance by providing discipline through broad market oversight.

A specific example of generator information being publicly disclosed can be found in the Australian National Electricity Market ("NEM"). To review this data, all one has to do is go to http://www.nemmco.com.au/data/marketdata.htm and click on "Market Management System (MMS) CSV Files." From there, by following the instructions, you can download the previous day's bids or the bids for earlier days to analyze in any manner you see fit. These bid data files also include information on unit availability and redeclarations of availability during the day. This allows the market participants themselves to monitor the market, producing greater faith in the integrity of the market.

---

16 FERC and the Energy Information Administration collect and disseminate information regarding most of the energy industries. Other information services, such as Dow Jones Newswires, gather information that is sold by subscription. Unlike the Government reporting requirements, news gathering services do not require the information provider to sign a certification or affidavit attesting to the accuracy of the information.

17 The National Weather Service River Forecast Centers website contains links to numerous regional river forecast centers [http://www.websites.noaa.gov/guide/government/nwsrfc.html].

18 Restructuring Today. "ISO Can Cut Off WSCC Data But Not EPA's". October 23, 2000. Page 3.

19 Letter from CAISO to Dennis Eyre, Director of WSCC, dated October 11, 2000.

Timely resolution of market problems is essential. By delaying disclosure, problems are not resolved through informed, fair, market-driven processes. They are investigated, through legal discovery mechanisms, and brought to FERC or the courts for resolution. Electric power markets are fast-paced and forward-looking. Delaying settlement over disputes where information is not forthcoming, sidelined by delayed disclosure rules, or altogether concealed from any scrutiny, will erode market confidence and ultimately increase costs.

D. Managing Forced Outages and Preventing Capacity Withholding

A common concern expressed by the merchant segment is that if the market observes that a facility is experiencing an outage, the owners will be unfairly punished in the market by paying high prices for replacement power. It is difficult to dispute the premise, but the issue should be examined more broadly before concluding that the "naked" merchant is being unfairly punished.

First of all, when all merchants are "naked" in the market — subject to full disclosure of generator-run status — none has a particular advantage over the others. If the market is constrained and faces diminished reserve margins, it is imperative for certain generating plants to stay on-line and available at or near full capacity. Historically, forced outages are low probability events. The risk of needing to buy high-cost replacement power provides the proper incentives to maintain plant equipment off-peak to ensure on-peak performance. Reserve sharing agreements and replacement capacity markets—not hiding generator forced outages from disclosure—are the appropriate mechanisms to insure against the risk of forced outages.

Unfortunately in many regions, market structures have been created that provide the opposite incentives. A generator can declare an outage in order to test market price response. With disclosure of generator run status information this type of market behavior would be more risky since others can observe the action.

Under current rules that permit concealment of "commercially sensitive" information, it is possible to withhold capacity without coming under the scrutiny of other market participants (including buyers). When system data is concealed, forcing outages, arbitrarily derating capacity, or simply withholding capacity from the market to observe market price response is more easily accomplished and in many cases is richly rewarded by higher market prices.

To allow concerns about punishment for low-probability forced outages to drive disclosure policy implies a willingness to accept a significant risk exposure to market manipulation that could otherwise be timely detected and addressed. Conversely, disclosure of a broad range of system information, including generator-run status will: (a) provide rational feedback to all market segments for improved system response, and (b) create disincentives for market participants to withhold capacity from the market for strategic reasons.

7. Dispelling the Fears of Revealing Generation Data

To assume that having generator status information would completely reveal a merchant's position (long or short) in the market is not true. One can only assume that the merchant may or may not be able to cover its position. But other merchants do not know what this merchant's position is solely by the status or loading of generators that it may own or have interests in. Only that merchant's books hold that information.

To accept this proposal, the industry must accept that all generators should reveal their run status in an open, non-preferential medium such as the Internet through OASIS. It cannot be an opt-in/opt-out choice. Generating entities must further understand that the value of this compromise is that it provides a necessary means for verifying the existence of full and fair competition and absence of market power in specific geographic markets. Failure to meet appropriate criteria for competition and continued abuse of horizontal market power will likely culminate in re-regulation of generation markets.

8. Authors and Contributors

Kurt J. Conger, Allen Mosher and Diane Moody
American Public Power Association

Charles Yeung
Enron Corporation

9. Sponsors

Paula S. Green
Deputy Superintendent
Seattle City Light Department

Joseph Krupar
Florida Municipal Power Agency

Ron Eachus, Chairman
Roger Hamilton, Commissioner
Joan Smith, Commissioner
Oregon Public Utility Commission

Mark Gerken, President
American Municipal Power-Ohio

Mike Green
Chelan County PUD

Generator-Run Status:
Position Paper Opposing Data Disclosure to the Market Within OASIS Phase II

January 29, 2001

Introduction

The purpose of this position paper is to present to the Electronic Scheduling Collaborative (ESC) an exposition on the reasons why generator run status should ***not*** be incorporated into OASIS Phase II or any other publicly available format. For the purposes of this document, it is assumed that generator run status includes the posting of both real-time information regarding the current online or offline status of a generating facility and any future outage plans regarding the generating facility.

In addressing the topic of posting generator run status, this document intends to discuss the following issues:

- Nature of the information under consideration
- Commercial sensitivity of the information under consideration
- WSCC EHV Data Pool project
- NAERO Compliance Report
- Generator Information is private property
- Anti-Competitive implications of publishing the information under consideration
- Pretense of common arguments in favor of publishing the information under consideration
- Natural Gas precedence for not publishing the information under consideration
- Implications of Posting Forecasted Information

The discussion that follows should provide an acceptable apology to substantiate the premise that generator run status should not be publicized via OASIS Phase II.

Background

On December 20, 1999, the Federal Energy Regulatory Commission (FERC) issued its Order 2000, effectively mandating the creation of Regional Transmission Organizations (RTO) in the United States electric industry. In a follow-up action on July 14, 2000, the FERC issued an Advanced Notice of Proposed Rulemaking (ANOPR) seeking proposals for how OASIS Phase II should be implemented. From the inception of OASIS as mandated in the original FERC Order 889, OASIS Phase II was expected to include not only standards for how transmission information is posted and transmission service is acquired, but also how electronic scheduling of transmission reservations is to be accomplished. Responses to the ANOPR are due to be filed at the FERC by February 15, 2001. In an effort to seek industry consensus regarding OASIS Phase II, the North American Electric Reliability Counsel (NERC) formed the ESC to respond to the

FERC ANOPR. As a result, the ESC has taken on the responsibility of addressing the many issues raised in the ANOPR.

One of the issues raised in the ANOPR is the posting of generator run status. On page 8 of the ANOPR itself, the FERC has stated that "The proposals should discuss whether … generator-run status information should be incorporated into OASIS Phase II." This issue, which has been raised on several occasions in the past, has not been resolved in the industry because it has historically resulted in heated debate to which neither consensus nor compromise has been reached. In order to address this issue in the ANOPR per the FERC requirements, the industry must attempt to reach a consensus opinion regarding disclosure of generator run status information.

Nature of Generator Information in a Competitive Market

As it is the objective of the ESC to develop standards regarding electronic scheduling, it is imperative to understand the nature of the components of an electronic schedule. While each of these components may be broken down into sub-components, there are three primary components to a physical schedule. The components are the generator, the load, and the transportation between the generator and load. To the extent that these components are utilized in the wholesale energy market, they fall under FERC jurisdiction. Of these components, FERC has only ordered open access to the transportation component - primarily because of its monopolistic characteristics. As yet, the FERC has not ordered access to retail loads - perhaps because such would likely be an infringement on state regulatory jurisdiction. Similarly, the FERC has not ordered access to generation. The reason for not ordering access to generation is two-fold. First, generation is the sole property of its owners and exclusive rights to such property will not hinder the development of a competitive market place. Second, in the post-888 market, generation is not a natural monopoly. Instead, the FERC has facilitated the development of a competitive generation market by establishing the rules necessary to reduce market power and eliminate the monopolistic nature of generation market share.

As a result of these cooperative actions by the FERC, generation has become a commodity in its own right and a reasonably liquid market for trading generation rights has developed. Owners of the bricks and mortar of the generation facility essentially have physical rights to the generation supply, to which they can therefore trade in the commodity exchange market. Marketing entities can take either long (buy) or short (sell) positions in the commodity market based on the expectation of the availability of the energy associated with the generation. As such, the owner of the generation itself essentially owns a position in the market equivalent to the capability of the facility, and any information associated with that generation is the sole property of the asset owner.

The nature of the position that the generator owner holds in the market is analogous to a market call[1]. When demand necessitates and/or market prices are higher than the unit's generation cost, the generator owner may "exercise" its rights to the asset (i.e. receive the energy generated) in order to sell energy into the market. When market prices are lower than its generation costs, the owner may choose not to exercise its rights to the asset and may either meet its demand obligations through market purchases or abstain from participating in the market altogether.

[1] CALL - the right, but not the obligation, to receive energy at a specific price.

Essentially, generation is a critical part of the owner's market portfolio[2]. For many generation owners, the share of their portfolio represented by generation assets may be extremely large as compared to the share of the trading assets (i.e. power purchases) in their portfolio. This may be because of business strategy or it may be because of regulatory requirement. Nevertheless, for entities, which are heavily weighted in favor of physical assets compared with financial and/or trading assets, disclosure of generation run status represents the disclosure of a significant portion of their portfolio. The next section describes the commercial ramifications this may have on such entities.

Commercial Sensitivity of Generator Information

Generators can represent a significant portion of the trading portfolio for its owner. As such, generator status also represents the current state of said trading portfolio. Publicizing this information therefore has significant commercial ramifications. Information associated with generator run status is the proprietary intelligence of its owner, and not for public consumption unless so desired by the owner. Furthermore, because the proposal is only for posting generator status (and not all trading positions), there arises serious inequity - if not anti competitive - implications between generator positions versus market positions.
To illustrate the commercially sensitive nature of generator status information, consider the implications of posting the complete books of all market players. For the time being, ignore pricing information (that will be discussed in the next section) and only consider relative market position (long, short, and by how much). Because everyone in the market would know the relative position of everyone else in the market, some would have the ability to gain an unfair advantage over others. It is unlikely that those who support publishing of generator run status information would consider or support the public disclosure of their own complete trading portfolio. In fact, the question should be asked whether there is a successful, liquid commodity market anywhere in the world that publishes this information. If not, the follow-up question should be why a significant portion of the wholesale power market should be exposed in this manner.

To solidify the position that generator status is, in fact, proprietary, commercially sensitive information, this document draws a comparison to the recent industry policy issue associated with distribution of NERC tags to all parties of the transaction. From its initial inception, NERC tagging, which contains much of the information required for electronic scheduling, has been considered to contain highly sensitive, commercial information. NERC tags not only contain source, path, and load information; but they also contain counter parties, revealing contractual relationships between market entities. In fact, many marketers feared that loads would see the availability of generating sources and bypass the "middleman" marketers - forcing them out of the transaction. As such, there has been an effort since the beginning to keep this information confidential, protecting the commercial positions the marketers may have taken with the generation owners. However, due to the way NERC developed tag submittal procedures, only one entity was allowed to submit the tag. Therefore, entities who were party to the transaction and who had financial obligations at risk if the tag were not submitted correctly did not always have access to the tag to ensure its accuracy. As a result, an effort was initiated to get the tag distributed to only those entities who were party to the transaction. This created significant polarization between those who wanted complete non-disclosure and those who wanted

[2] PORTFOLIO - the combined list of supply assets (whether physical generation or power purchases) and demand obligations (whether physical load obligations or power sales obligations).

disclosure to those who were party to the transaction. Even then, very few tried to say that the information was not commercially sensitive and even less supported having the tags disclosed to the public at large.

The correlation with generation run status is very clear. Posting of generation run status does much more than publicize the relationship between marketers and generators, it publicizes the availability of the market supply itself and does so on an entity by entity basis. Combined with other intelligence information, this can have no other result except to influence market pricing.

WSCC EHV Data Pool Project

In an effort that is concurrent with the ESC efforts, the WSCC has been struggling with the issue of data confidentiality within the EHV Data Pool project. The current expectation is that the EHV Data Pool would be used not only by Security Coordinators and Control Areas, but also by regulators and market monitors as a means of "policing" market entities. Because of the Freedom of Information Act that governmental agencies are subject to, market entities are dealing with concerns that regulatory access to the EHV Data Pool would disclosure proprietary information to the general public. Therefore, some entities have indicated that they will not participate in the EHV Data Pool as a result. To address this concern, the WSCC is proposing that EHV data would be categorized such a way that all of the information would be available to the Security Coordinators and Control Areas but only the non-confidential information would be available to the public.

NAERO Compliance Report

Perhaps of greatest significance when it comes to building consensus on the issue of determining the commercial sensitivity of generator data is the current direction of NERC itself. As part of its transition towards NAERO3, NERC has posted for comment its draft report from the Compliance Task Group4. Because this report is already in NERC due process, its finalized form should represent industry consensus regarding the issues it addresses. One of the issues it addresses is data confidentiality. Addressed in Section 5.03, the Compliance Task Group draft report clearly considers all generator data to be confidential in nature. According to the report, "all data submitted to an RRC [Regional Reliability Counsel] by a Participating Compliance Entity in accordance with the RRC's enforcement protocols shall be treated as confidential data by the RRC, and shall not be disclosed to any third part without prior written consent of the Participating Compliance Entity." Assuming this report survives NERC due process in tact, industry consensus will have agreed that all data submit by compliance entities (which generator owners will be compliance entities) must be kept confidential unless the owner of the data has granted previous consent. Clearly, generator run status would fall under the umbrella of this portion of NAERO compliance and should be considered as significant input into the consensus building for this portion of the FERC ANOPR response.

[3] NAERO - North American Electric Reliability Organization, the proposed mandatory compliance successor to NERC.

[4] http://www.nerc.com/naero/transitiondocs.html

Generator Run Status is Private Property

The previous sections described the nature of generation assets as it relates to the market place and summarized the commercial sensitivity of information regarding those assets. This section focuses more specifically on the property rights aspect of information associated with generator assets. A generating facility is the private property of its owners, resulting from millions of dollars of financial investment. As such, information associated with that investment is also private property. There is already a precedent for providing information regarding that investment for the purposes of maintaining system reliability. This is done as much for the benefit of the asset owner as for anyone else. The asset owner cannot deliver the product without a reliable transportation system and the transportation system cannot be reliably maintained without this information. Disclosure of this information to reliability entities bears no risk of financial harm to the generation owner - especially if disclosed under the umbrella of confidentiality agreements. However, disclosure of this information to the general market place takes things beyond the need for reliability purposes and exposes the generation asset owner to the potential of significant financial harm. As such, disclosure of generation information to the market place has the potential to devalue the asset and essentially represents a confiscation of a portion of the asset itself. The implications of confiscation of private property are fairly clear.

Anti Competitive Implications of Publishing Generator Run Status

This section will deal with the commercial implications of publicizing generator run status. It is the firm position of this paper that disclosure of generator run status information will create a non-comparable, if not anti-competitive, market situation.

Generator status represents the state of the portfolio of its owners. However, it does not represent a disclosure of all of its owner's portfolio, just the state of its owner's physical generation assets. Some will use this argument as justification in favor of disclosure (i.e. it doesn't disclose the full portfolio), but this document uses this argument as precisely why it is non-comparable and anti-competitive. Disclosing generator status ONLY discloses a portion of the portfolio. In fact, depending upon the relative size of an entity's physical portfolio compared to its trading portfolio, different percentages of the portfolio are exposed. For those entities that have a very large trading business and a very small physical asset base, the exposure is relatively small. For those entities that have a very large physical asset base and a very small trading business, the exposure is extremely large. By definition, this is non-comparable, and could be considered anti-competitive as well. The end result is that some entities will have a competitive advantage over other entities. Those entities will have the ability to game the market and, in some cases, even be able to exercise market power over other entities in the market. The result is the potential for extreme short-term volatility in the market whenever there are sudden changes in generator status. Nearly without fail, this volatility will be at the expense of the generation owners in favor of the rest of the market. In fact, most of the sponsors of this document have had personal experience with these short-term price fluctuations resulting from commercially sensitive information being exposed to the market. Most nuclear generation facility owners can attest to this fact because nuclear generation status is dislosed by federal mandate for the safety of the general public. Some may argue that generation owners who have this information can use this information to their own benefit. This document declares that because it is proprietary information that belongs to the generation owner, the owner is entitled to use the information for his/her benefit and such is neither non-comparable, unfair, nor anti-competitive. Likewise, some

may argue that disclosure of this information says nothing about how well the physical asset is hedged and therefore an entity that is properly hedged should be willing to accept this disclosure. Both of these pretenses will be addressed in the following section of this document.

Finally, the anti-competitive nature of disclosing generator run status information actually goes beyond mere disclosure of market positions because of related activities at the FERC. The FERC has ordered all developing RTOs to develop procedures for internalizing and dealing with transmission congestion. As such, many RTOs are exploring the possibilities for how this can be accomplished. One of the most predominant methodologies for dealing with congestion is the use of Locational Marginal Pricing (LMP). LMP essentially allows for the calculation of spot transmission pricing around a point of congestion. It can be an excellent tool for managing congestion, because it provides pricing signals associated with the congestion. However, what LMP also does is reveal the market price of incremental generation on a bus by bus basis. Therefore, with appropriate analysis, it is sometimes possible to determine a particular generator's marginal bid price. By itself, this can be a disturbing price revelation for generating owners, but the congestion management benefits outweigh the commercial concerns. However, when combined with generator run status, the generator owner is at risk not only to price disclosure, but portfolio position as well. In essence, not only is the state of the portfolio partially disclosed, but the pricing of the portfolio is exposed as well. The pretense that this information will even further increase congestion management will be addressed in the next section.

Pretense of Common Arguments for Disclosing Generator Status

This section will address several of the most common arguments used by those in favor of disclosing generator status information, including:

Market Information Should Be Disclosed Comparably
If Properly Hedged, Generator Owners Should Not Fear Disclosure
Disclosure Increases Congestion Risk Management

Market Information Should Be Disclosed Comparably. This argument centers on the fact that generation owners know the status of their facilities and that the rest of the market does not, thus resulting in a non-comparable market situation. The source of this argument is most likely rooted in the non-comparability standards associated with transmission access. The FERC is very clear that unfair transmission information can be used to create market power and manipulate the markets. Because transmission is a natural monopoly, FERC believes - and most people agree - that this information should either (a) be kept from the market or (b) be universally disclosed to the market. Those who support disclosure of generator status extrapolate this position into the realm of the generation market. However, therein lies the fallacy of the argument. According to market power assessments made by the FERC to allow generator owners to sell at market based rates; generation availability is not monopolistic. It is, by FERC creation, a commodity. The generation market is intended to be and is generally accepted to be an open market rather than a monopoly. Therefore, information associated with generator status is the proprietorship of the generation owner. As such, the premise that generator status is "market information" that should be publicly disclosed on a comparable basis is false.

Properly Hedged Generator Owners Should Not Fear Disclosure. This is simply an argument that has no relevance to the issue at hand. Whether or not a generation owner's position is properly hedged has no bearing on the policy implications of disclosing his/her proprietary information. Even if an asset is properly hedged5, there is a constant market effort to do better than the hedge. Hedging a trade is done primarily through financial means and is intended to protect against price volatility. Sometimes this can be accomplished through physical trades, but essentially the result is financial. As an example of a simple hedge, a short (sell) position can be hedged with a call option and a long (buy) position can be hedged with a put option. Essentially, the hedge locks in a WORST CASE scenario for the portfolio. However, the trader has every incentive in the world to beat the hedge. Every trader in the business knows and understands that if the rest of the market knows and understands his/her position, the trader will have difficulty beating the hedge - especially if his/her market position is exposed to the market in an unfair proportion to those of his/her competitors. Compare that to a physical hedge. A physical hedge is not made to protect against price volatility, but to protect against the state of the physical assets. Unlike a trade, whose state is fixed but whose price may or may not be certain, a physical asset has a probability of state and a probability of price. Essentially an asset owner has to hedge against both price and state. Also, there is always some minute probability that all assets are unavailable, meaning that it is never possible for a physical asset to be 100% hedged without extremely large reserve levels requiring extremely large investments (compared to hedging of trades, which only requires taking additional option position). For the regulated utility, state regulators often set the limitation on the level of physical hedging allowed. The result is that outages will result in price fluctuations. Therefore, physical asset owners must also hedge against price fluctuations - thus the argument presented here that generation owners should not fear disclosure because they should be properly hedged. However, ASSUMING state regulators allow price hedging for the physical assets (in itself a fairly big assumption), there is still a fiduciary responsibility to "beat the hedge" and disclosure of generation status adversely affects the marketers ability to do so. Finally, for regulated generation owners, the assumption that state regulators allow price hedging is not necessarily a good one. Unlike deregulated market entities, which have the choice to enter into transaction based on expectation of profitability and risk, regulated utilities have an obligation to serve load - even load deemed to be unprofitable or risky. Thus the regulatory compact. In exchange for a guaranteed revenue level that both covers expenses and provides a reasonable return on equity, the utility must serve all load and the state regulatory commission has final approval on all expenses. As such, regulated utilities are not always afforded the flexibility of being able to enter into the complex financial hedges available to deregulated marketers. This results in a potential exposure to short term price fluctuations, to which the utility is obligated to protect against in any way possible, including but not limited to opposing market policy that may leave its regulated, retail customers exposed to greater price volatility.

Disclosure Improves Congestion Risk. The argument that disclosure of generator run status will improve congestion management is a tenuous argument. It is true that generator status contributes exclusively to flows, which create congestion - meaning that knowledge of generator status can help predict congestion. However, it is unlikely that real-time knowledge of generator status will increase the ability of marketers to manage their risk - primarily because of efforts already underway to do so through other means. The true measure of congestion will be the interface/flowgate limits (which should be posted) and the current net interchange schedule (which the ESC wants posted). Furthermore, generator status alone will not give a true indication of flowgate congestion, because there are so many more variables that also contribute to

[5] HEDGE - typically a financial instrument that limits loss exposure under unfavorable conditions.

congestion. It is not reasonable to believe that all of the variables will be available to the marketplace or would be more useful than the information for the flowgate itself. In comparison to generator status, these provide a much better indicator of expected congestion. Finally, under Order 2000 all RTOs must have a market-based method of dealing with congestion, meaning that they will have to implement some form of market based redispatch. It is highly probable that the RTO proposals developed will make any incremental benefit received from generator status negligible, depending on the model they adopt. Many of these RTO proposals will likely be based on LMP, which provides a market-based pricing signal associated with real-time congestion. Therefore, when weighing the benefits of disclosing the information vs. the detriments of disclosing the information, the primary benefits may actually be negligible because those benefits can be achieved through other means.

The Real Reason for Disclosure. So what exactly are the real benefits for disclosing generator run status and do they perhaps provide some insight into why there is a movement by some parties to have the information disclosed? Disclosing of generator run status provides the market with critical information about its competitors. To believe that this can harm the owner of those assets, you must be willing to accept the fact that the wholesale power industry is not always an efficient, liquid market. You must believe that situations exist in which there are not enough market players to prevent exploitation. Unfortunately, experience has shown that this can be the case. During the summer months, when demand is at its highest levels and discretionary supply (i.e. available to the wholesale market) is at its lowest levels, the North American transmission grid is virtually shut down by congestion. This often leaves high demand areas cut off from high supply areas, giving available supply in those areas near market power. Keeping proprietary generation information from reaching the market is very often the only defense against exploitation.

Natural Gas Precedence

Are the apologies presented in this document sufficient reason for not disclosing generator run status? The sponsors of this document believe so, but they are also willing to take the discussion one step further. The natural gas industry is generally considered by the FERC and by many market participants as being mature, liquid, stable, and the ongoing model for the deregulation of the electric industry. Therefore, since many of the proponents of disclosing generator run status are also major players in the natural gas industry, it seems prudent to examine the natural gas industry to see if there is a precedence there for disclosing this information.

The natural gas equivalent to an electric generating facility is a drilling platform or well. The natural gas equivalent to generator run status would therefore be the drilling status of the wells. Is there a natural gas precedence, therefore, for publishing this information? Actually, the precedence is the exact opposite, because there is no published information that describes in real time the status of the drilling platforms and wells - nor is it likely that the major oil and gas players would want this information published. Furthermore, due to the nature of the gas industry, it is unlikely that this information would have a significant impact on the market. What the gas industry does have, however, is a weekly storage report. Unfortunately, there is no electrical equivalent to the storage report. First, it is an indication of available ENERGY, not an indication of available CAPACITY. Natural gas can be stored; electricity cannot be stored. The storage report indicates natural gas that has already been "generated" (i.e. processed), is being stored, and is ready for public consumption. By contrast, electric capacity is always

instantaneously equal to electric demand, which can dramatically change in real time. Therefore, there is no way to indicate the amount of electric supply that is ready for public consumption without certain availability assumptions. Second, the storage report is more of a mid-term indicator of supply, not a real time indicator of supply. The closest electrical equivalent would be a projection of planned maintenance (discussed later in this report), but even that would be flawed because not only would it be subject to changes in maintenance schedules, but it would also neglect economic decisions to commit and de-commit generating facilities. Finally, the storage report is an aggregate report, not a well by well summary of production. Unlike the proposed disclosure of generator run status, the natural gas storage report can not isolate individual market participants for targeted exploitation.

The gas industry has matured and become liquid without the equivalent of this information being disclosed. As such, the natural gas industry has set a positive precedence for the electric industry to follow. The conclusion that can be drawn is that mature, open markets can develop without disclosing this level of proprietary information. The electric industry can mature without it as well.

Implications of Posting Forecasted Information

Most of the discussion thus far has been centered around the posting of real time generator status. Although many of the above arguments also hold true for posting forecasted information, this section will focus on the specific case of posting forecasted generator information. The most significant difference between posting real time information vs. forecasted information is the fact that posting of forecasted information provides a greater risk of market manipulation with an even smaller expectation of benefit.

Because it is forecasted information, there is a significantly greater risk of market manipulation from the additional available market reaction time. While there is a fairly nominal risk of market manipulation from the posting of real time generator status, there is even more risk when the market has greater time to contemplate the implications of the information provided. Furthermore, it is not just the rest of the market manipulating the asset owner that is at stake. There is also significant risk of the asset owner itself providing false information for the sole purpose of manipulating the market. This can not only affect the market, but could affect system reliability as well.

Finally, because it is forecasted information, the benefits received are flawed and could lead to further market distrust. Unplanned outages can occur unexpectedly, but so can changes in planned outages as well. A generation owner may respond to market pricing signals by changing maintenance schedules. As such, what may be published at a forecasted outage may or may not materialize, which can lead to accusations that the generation owner is being untruthful for the purpose of manipulating the market. While it is possible that this can happen, there is no way to determine whether the change in forecast status was a result of legitimate business decisions or direct market manipulation.

By contrast, keeping forecasted generator status information confidential between the owner and the reliability organization ensures that the reliability agents are being provided with the most accurate information possible.

Conclusions and Sponsors

Based on the discussions herein, the sponsors of this document believe that posting of generator run status for public consumption should not be incorporated as part of OASIS Phase II. The following are the sponsors of this document:

Joel Dison
Project Manager
Southern Company Services, Inc

James Eckelkamp
Wholesale Power Dept.
Carolina Power & Light

Eduardo DeVarona
Sr. Power Coordinator
Florida Power & Light, Co.

Bob Ebrick
Manager
El Paso Energy

Scott Coe
Manager, Scheduling Coordination
Bonneville Power Administration

Jeff Lambert
Sr. Power Marketer
PPL EnergyPlus

Michael Hall
Certified System Operator
NCEMC

Stephen Beuning
Sr. Operations Consultant
Xcel Energy Marketing

Bob Stegmeier
Sr. Power Scheduler
Aquila Energy

Public Comments
Generator-Run Status Position Papers

-----Original Message-----
From: Prowse, Dan [SMTP:dcprowse@hydro.mb.ca]
Sent: Friday, January 26, 2001 5:01 PM
To: 'estf@nerc.com'
Cc: Cormie, David; Hunter, Kelly; Wojczynski, Ed; Reznichek, Karl; Clendenan, Judy; Poff, Blaine; Koschik, Wally
Subject: Manitoba Hydro Position Opposing Disclosure of Generator Run Stat us in OASIS Phase 2

Postion forwarded by,
Dan Prowse
Manitoba Hydro
Support Engineer, System Control Department
Phone 204-487-5382

Manitoba Hydro Position Opposing Disclosure of Generator Run Status in OASIS Phase 2

Manitoba Hydro staff strongly support the position of non-disclosure of generator run status (GRS) information. We don't find anything in the proponents position that would allow for compromise.

We feel the proponents (mainly large sophisticated marketers) of this issue have very little to lose and everything to gain by having disclosure. They have complex trading portfolios usually with only a small proportion dependant upon actual generation assets. Disclosure of their GRS would reveal little about their market position. However as a market participant whose asset portfolio is almost completely physical (i.e. we have no financial assets in our portfolio) Manitoba Hydro cannot hide behind a complex portfolio and therefore is much more exposed to the risks inherent in revealing GRS. A sophisticated competitor could combine publicly available transmission outage information with GRS info and gain almost complete insight of our market position to our disadvantage.

We believe that publishing GRS will only be treating the symptoms of the fundamental problem that exist in certain markets that have insufficient generation supplies relative to load. In these markets we agree that there is the potential for some generators to exert market power. However the solution to that is not to confiscate the property (GRS) of the generators but is to mandate adequate planning reserves as is the case in MAPP. With adequate generation resources available relative to load, market power issues raised by the proponents is a non issue as FERC only licenses market participants who demonstrate that they don't have market power. If the situation in a particular market changes such that a market participant does have market power the remedy should be against that participant. Asking all generators in all markets to reveal GRS won't remove the potential for market power abuse in markets with insufficient generation.

We also disagree with the argument that making GRS available to the marketplace is necessary to ensure regional reliability. In MAPP it has been demonstrated that reliability can be maintained without compromising commercial interests through public disclosure of GRS info.

Allen Mosher
Director of Policy Analysis
American Public Power Association
2301 M Street NW
Washington, DC 20037
Voice: 202-467-2944
Fax: 202-467-2992
amosher@APPAnet.org

Dan,

I suggest that you look again at the list of supporters of disclosure, which includes municipal systems, municipal joint action agencies, state regulators, and one large power marketer/generator.

Speaking for the state/municipal segment of the market, APPA has a number of large members, but most APPA systems are small municipalities that buy the bulk of their energy requirements. We are in the business of serving our loads. We also generate power - using our own physical assets - and when we have surplus generation, selling it in the bulk power market. While there may be exceptions, APPA members are not typically involved in the marketing of power based on a financial asset portfolio. We sell power backed by physical resources. Most APPA members are transmission-dependent utilities as well, and when they operate a control area, it tends to end at the point of interconnection with the regional utility that surrounds the municipal system. For us, the behavior and performance of the bulk power market and the bulk electric system often has a level of behavioral opaqueness and incoherence that larger market participants probably find difficult to understand.

Thank you for your consideration of these views.

TO: NERC Electronic Scheduling Collaborative (ESC)

FROM: Exelon Corporation
RE: Generator-Run Status Position Papers

DATE: JANUARY 25, 2001

COMMENTS OF Exelon Corporation.

Exelon Corporation is pleased to present these comments in response to the NERC ESC request for Comments on the "Generator-Run Status Position Papers.

Exelon Corporation, one of the nation's leading providers of energy services, is the company formed from the merger of Unicom and PECO Energy. Exelon operates in MAIN & MAAC Reliability Regions, markets energy throughout North America, and owns and operates in excess of 16,500 megawatts of nuclear capacity.

Exelon Corporation strongly agrees with the position taken by the authors of the **Position Paper Opposing Disclosure of Generator Run Status Within OASIS Phase II.** Exelon as the largest owner operator of nuclear capacity North America is required by federal mandate to disclose nuclear generator status, and as such has endured market manipulation, price fluctuations, and volatility.[1]

We believe generator status information is proprietary information that belongs to the generator owner, the owner is making the investment and taking the risk of bringing a product to market, the owner is entitled to use the information for their benefit and is neither non-comparable, unfair, nor anti-competitive.[2] Exelon believes that generation (by FERC definition) is a commodity that generation owners freely trade (or not trade) on the open market. As such the premise that generator status is "market information" that should be publicly disclosed if false.

In reviewing the **Paper Supporting Data Disclosure to the Market Within OASIS Phase II** we were concerned with much of the logic and assumptions used in order to support the paper's position. The paper implies that disclosure of generator run status will enhance reliability but there is no basis for this statement. Those charged with maintaining security of the network presently receive the data.[3] The other reason for requiring disclosure of generator run status is to be able to perform market monitoring. Yet, in Order No. 2000, the Commission assigned this function to RTOs. A neutral party can allay any fears of withholding or other concerns while protecting the confidentiality of the data, especially in real-time. The paper states that the electric power industry has been characterized by "violations of Standards of Conduct", "environment ripe for collusion", Exelon Corporation would endorse a FERC initiative to enforce existing rules to eliminate any potential or existing violations. What this all boils down to is that those supporting disclosure of generator run status simply want market intelligence for their own

[1] Those supporting disclosure of generator runs status admit this is a problem (Jan. 2, 2001 paper at 8).
[2] Of course Exelon makes generator run status and all other information needed for system security available to control area operators, security centers and Security Coordinators.
[3] The one, extreme example mentioned in the paper about an islanding incident does not make a credible argument that generator run status would increase reliability. First, if the transmission operator had difficulty determining that islanding had occurred (a highly unlikely conclusion on the part of the authors), there is far less likelihood that individual generators would arrive at the correct conclusion. Second, the authors appear to assume that under such a situation generators would take uncoordinated action rather than work with the control area operator or security coordinator. This would create a situation more adverse to maintaining reliability.

use. This should not be allowed. ~~Exelon is of the opinion that the authors of the paper are attempting to coerce lawmakers into requiring proprietary information be made public in order to manipulate and control wholesale energy markets throughout North America.~~

Exelon does not see an area of compromise between these positions.

Thank you for the opportunity to offer comment in this matter.
Questions regarding this document should be addressed to John Blazekovich at john.blazekovich@exeloncorp.com

Eric Little
Federal Regulation and Contracts
Southern California Edison
PAX 26607
(626) 302-6607
Eric.Little@sce.com

Southern California Edison submits the following comments on the draft position papers regarding disclosure of generator run status within OASIS Phase II dated January 9, 2001.

While SCE supports the disclosure of generator run status as detailed in the position paper, "Generator Run Status: Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II" (herein referred to as "supporting paper"), SCE does not believe that such disclosure should occur through OASIS in real-time. We believe that a delay in the disclosure of such information of approximately one to two weeks would strike a reasonable balance between making valuable information available to all market participants without contributing to potential market abuse, which could occur with real-time dissemination.

SCE agrees that the operators of transmission for reliability purposes must know certain market information. However, this can be accomplished by means other than a complete release of market information. Where such asymmetry of information is present, regulations may be put in place to prevent the anti-competitive use of such information. For example, in the California wholesale market, there are very strict regulations that prohibit the transfer of information from operational personnel to scheduling personnel. This arrangement would preclude the argument of system reliability and asymmetrical information.

While we further agree that more information is beneficial to competitive markets as proposed in the supporting paper, SCE believes that the supporting paper is flawed in that it assumes that the leak of information to participants asymmetrically is more damaging to the market than a symmetrical release of information. In cases where market power has been found to exist, such information can become a liability to the market. While we do agree that the selective release of information can be damaging to the market, we cannot conclude that symmetrical release of information in all instances would necessarily benefit the market.

Finally, the supporting paper proposes that release of generator run status will "discipline" the market. While this is a compelling argument for the release of data, even a prompt release of data, it is not a compelling argument for real-time release of such data. Precedence of a reasonable delay in reporting has been established in 90 FERC 61,316 in which FERC ruled that release of individual bid data in as little as one month does not protect the commercial sensitivity of the data. One could similarly conclude here that while generator run status is not as commercially sensitive as bidding behavior, the real-time release of such information is not in the public interest.

On the other side of the coin, SCE does not believe that complete withholding of such data from the market is in the best interest of the market. In particular, SCE is not convinced by the circular reasoning in the white paper titled, "Electronic Scheduling Collaborative Position Paper Opposing Disclosure of Generator Run Status Within OASIS Phase II" (herein referred to as "opposing paper). The opposing paper states that generator run status should not be released, as it is the property of the generation owner. It is without merit to claim that the very issue that is being considered (property rights of information) is the very reason that the issue should be resolved in a particular manner (in this case, denial of information). This presumes that property rights have been assigned despite the fact that property rights are the issue in question.

Additionally, the opposing paper claims that dissemination of generator run status creates "inequity – if not anti competitive – implications between generator positions versus market positions." First, this argument presumes that more information would be known by load about the position of the generator

than the generator knows about the load. This is untrue. Every wholesale electricity market in the United States has a balancing market. This market is used to true up the net short or long position of load serving entities. This position is then made known to the market in general when the system operator solicits bids to match the load. Secondly, this argument presumes that if information is made known to the load, the load could and would exercise monopsony power. This argument is not supported in evidence.

For the aforementioned reasons, SCE supports the release of generator run status data with a sufficient lag of one to two weeks and therefore, necessarily opposes real-time release of such data through OASIS.

James R. Stanton
Manager of Market Policy
Calpine Central, L.P.
700 Louisiana, Suite 2700
Houston, TX 77002
713-830-8694
jstanton@calpine.com <mailto:jstanton@calpine.com

After reviewing the two opposing viewpoint papers posted on the NERC website, it seems obvious to us that generator run status should not be a part of the OASIS Phase II information. The benefits to the end use customer concerning energy price and the broad availability of the ancillary services will come from a healthy market. To allow the markets to function, to facilitate the movement of power from the most cost efficient generation to the most price sensitive end users, should be one of the overriding principles guiding any changes to the control of the electric grid. To consciously disable a portion of that market by putting generation at a disadvantage in relation to other market participants hurts everyone. Granted, generator run status should be available to the Regional Transmission Organizations and the Independent System Operators. Playing a part in the reliability of the system is a role we readily embrace. However, there is no need to have the status of privately owned generation facilities available to all market participants. The products of these facilities are traded in an open market. For that market to function properly, to allow the benefits open competition to accrue to the end users of the energy, it should not be skewed by an unbalanced availability of market sensitive data.

Jeff M. Klarer
Power Marketer
Wisconsin Electric
231 W. Michigan Street
P.O. Box 2046
Milwaukee, WI 53201
Phone: (414) 221-4350
Fax: (414) 221-4210
E-mail: jeff.klarer@wepco.com

Comments Opposing the Disclosure of Generator Run Status Within OASIS Phase II

Introduction:

The purpose of this paper is to indicate Wisconsin Electric's opposition to the disclosure of generator run status as part of OASIS Phase II or any other publicly available format, and to point out problems with the arguments made by proponents for disclosure of generator run status. Wisconsin Electric strongly believes that generation information is proprietary information and that public disclosure of generator run status would unfairly harm the competitive position of load serving entities holding the rights to generation resources while failing to provide the purported benefits of disclosure.

Purposes of Generator-Run Status Information:

Section 6 of the *Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II* lists the four main reasons for disclosure of the information as *System Security Assessment, Benefits for Reliability, Market Discipline,* and *Managing Forced Outages and Preventing Capacity Withholding.*

In the section on *System Security Assessment*, the proponents for disclosure acknowledge that the generator run status information that

they seek is already made available to the entities responsible for overseeing the safe and reliable operation of the electric system. Their contention that the standards of conduct are not adequately monitored may be viewed as justification for improved or increased monitoring by the FERC, but not justification for the release of competitive confidential information.

The assertion that disclosure of generator run status will provide *Benefits for Reliability* is tenuous at best. In the example of the merchant in the Midwest that noticed its generator was rotating at a speed equal to a system frequency of 62.5 Hz, the assertion is made that if the merchant had access to generator run status for neighboring units, this situation would not have continued unresolved for a few hours. In reality, this information would not have assisted in determining that breaker action had created an island in the system. The primary piece of information indicating the existence of an island problem, was the high system frequency, which was already available to the merchant. It is also argued that generator status and output can directly affect transmission transfer capabilities. Although this is true, many other factors can impact transmission transfer capabilities. As stated on page 8 of the *Position Paper Opposing Disclosure of Generator Run Status Within OASIS Phase II*, "It is not reasonable to believe that all of the variables will be available to the marketplace or would be more useful than the information for the flowgate itself." The proponents of disclosure state on page 2 of the *Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II* that "We do not view the posting of other data (such as the net flows over commercially significant flowgates) as a good substitute for generation run status data." The fact that the proponents of disclosure do not feel that access to the data that provides the best overall picture of system reliability is as important as access to generation run status data indicates that the desire for this information is not related to reliability. Finally, as stated earlier, generator run status information is already available to the necessary entities that oversee system reliability.

In their discussion on *Market Discipline,* the proponents for disclosure attempt to argue that posting of generator run status information would enhance market performance by providing discipline through broad market oversight. What the proponents for disclosure fail to recognize are that the CAISO was correct in its assumptions that full disclosure may actually result in greater abuse of market power. If a generator has knowledge that its competitors' generating units will be unavailable, they would have an even greater ability to increase the price at which they would be willing to sell power due to the fact that the level of uncertainty of actually having their bid accepted would be reduced. Knowing the real time status of all generating units would provide a significant incentive to individuals having the rights to the available generation to increase their offer price to the detriment of the individuals needing to purchase power on the real time market. This would especially be true in areas where transmission constraints result in limited access to generation. This fact is acknowledged by the proponents for disclosure on page 4 of the *Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II* in their discussion regarding the *Pretense of Fully Competitive Generation Markets*. The assumption that a generator would not raise its price because market participants would be able to identify the plant from which it is supplying the power ignores the basic tenets of supply and demand and the profit motive. Furthermore, the proponents for disclosure state on page 4 of the *Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II* that "…forecasts can be unreliable and may themselves be manipulated for strategic reasons." The belief that broad market oversight would not prevent a participant from trying to manipulate the forward market to their advantage but would prevent a participant from trying to manipulate the real time market is inconsistent.

The arguments that *Managing Forced Outages and Preventing Capacity Withholding* will be improved by full disclosure also have significant problems. Wisconsin Electric agrees with the proponents of disclosure that forced outages are low probability events and the risk of high-cost replacement power provides an incentive to maintain plant equipment so the generator is available when needed; however, the argument that disclosure of generator run status data will somehow change the risk of a forced outage does not make sense. Legitimate forced outages will continue to occur regardless of data disclosure. The argument that the market structures in many regions have provided the incentive for a generator to declare an outage in order to test market price response would seem to indicate that generators in some areas are intentionally misrepresenting unit availability. This phenomenon, if it exists, is totally unrelated to forced outages but could be related to the intentional withholding of capacity. Furthermore, this argument provides greater support for changing poor market structure than it does for requiring full disclosure of generator run status data. As stated earlier, full disclosure of generator run status data would not prevent individuals from attempting to maximize their profit. In fact, full disclosure in regions where market structures do not provide incentives for a generator to declare an outage in order to test market price may have a negative impact on both price competition and reliability. If a generator can not be assured of confidentiality when providing information to the entities that oversee system reliability, they may actually have the incentive to provide inaccurate information that may have negative consequences for the safe and reliable operation of the system.

On page 9 of the *Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II*, proponents for full disclosure state that "… if the market observes that a facility is experiencing an outage, the owners will be unfairly punished in the market by paying high prices for replacement power. It is difficult to dispute the premise, but the issue should be examined more broadly before concluding that the "naked" merchant is being unfairly punished. First of all, when all merchants are "naked" in the market – subject to full disclosure of generator-run status – none has a particular advantage over the others." Whereas the proponents for full disclosure acknowledge the harm that disclosure can cause to the generation owner, they inaccurately characterize the situation as not being a disadvantage because all generation run status data is available in the market. The disadvantage arises from the fact that only market participants that have generation are being forced to provide information to the market place. The fact that the real-time market position of all market participants is not fully disclosed arbitrarily disadvantages those participants with generation.

Conclusions:

It is the belief of Wisconsin Electric that full public disclosure of generator run status would unfairly harm the competitive position of load serving entities holding generation rights. As a result of the disadvantages to market participants with generation and the fact that the purported advantages of full disclosure do not exist, Wisconsin Electric strongly opposes the disclosure of generator run status within OASIS Phase II.

Name: K. Pitchell
Organization: Independent Electricity Market Operator (IMO)
Phone#: 905-855-6115
E-mail address: kim.pitchell@theimo.com
Type: ISO, SC, CA

Document: Generator-Run Status Position Papers – Jan 26, 2001

Comment:

From a reliability point of view, the IMO does not foresee any concerns arising from the omission of Generator Run Status from OASIS II. This assumption is based on the premise that all Control Areas, ISO's and Security Coordinators have adequate generation information available to them for their assessments. Generation owners should have no concern with supplying that information to the respective scheduling/reliability/security entities a party to the confidentiality agreements.

Kurt Conger
EXS Inc.
Woodinville, WA
(425) 497-1133
Mobile (425) 444-3149

Rebuttal of Position Paper Opposing Disclosure

Each of the following sections identifies an argument appearing in the Paper Opposing Disclosure of Generator Run Status Information and provides a brief rebuttal.

1. "Commercial Sensitivity of Generator Information"--Analogies:
   In this section, at the end of first paragraph, the question is posed "whether there is a successful, liquid commodity market anywhere in the world that publishes this information." The supporting position paper points out the Australian National Energy Market (NEM) discloses this information. A similar situation exists in the England & Wales ("E&W") market, where bid data is available by generating unit one (1) day after bids are submitted (albeit, there is a charge for the data in E&W, unlike in Australia where the data is free). Separate subscriptions are also available for generator availability data, including minimum, average and maximum availability each day. To subscribe to the E&W data you simply go to http://www.esis.co.uk/index2.html and then register and go through the subscription process. Notwithstanding data disclosures, these markets continue to function, and have not collapsed in the face of open information policies. In these international electricity markets one does not see the public pricing and reliability concerns that, for example, one sees in the California market.
2. "WSCC EHV Data Pool Project:"
   Regardless of the California ISO decision to withdraw disclosure of information to WSCC, Section 352.5 of the California Public Utilities Code recently signed into law by the Governor now requires daily posting by the California ISO a list of all non-operating generating plants. See http://www.caiso.com/docs/2001/01/25/2001012508442613704.html.
3. "NERC Compliance Report:"
   Whether NERC decides to disclose information for purposes of compliance and enforcement is immaterial to whether another industry group, regulatory body or government agency determines that disclosure is in the public interest. This role of NERC or NAERO has a different purpose and need not be confused with other legitimate purposes of disclosure. NERC's activities will not be adversely affected by disclosure for regulatory and public interest purposes. That the NERC requirements and proposed disclosure requirements share the same technology for data interchange is synergistic to the extent that both tasks can be performed with the same hardware and software.
4. Generator Run Status as Private Property:
   Characterizing disclosure of Generator Run Status as a "confiscation of private property" is an attempt to build on the fallacy that there can be no public interest purpose served by disclosure to the public of information about privately owned assets. Clearly this characterization has been rejected by regulators and the courts in many instances, and not just in the electric industry. As pointed out in the paper supporting disclosure, precedents for public disclosure are provided. FERC has authority under 16 USC Sec. 825h ("The Electric Consumers Protection Act of 1986") as follows:
   "The Commission shall have power to perform any and all acts, and to prescribe, issue, make, amend, and rescind such orders, rules, and regulations as it may find necessary or appropriate to carry out the provisions of this chapter. Among other things, such rules and regulations may define accounting, technical, and trade terms used in this chapter; and may prescribe the form or forms of all statements, declarations, applications, and reports to be filed with the Commission, the information which they shall contain, and the time within which they shall be filed."
   Clearly the desired policy of the opponents to disclosure goes far beyond the scope of this debate. Matters of regulatory authority and determining what is in the public interest are best handled by Congress and the Courts. And for now sufficient Statutory authority rests with FERC to require

disclosure of generator information.

Ruckelshaus v. Monsanto Co., is the leading case on disclosure of potential trade secrets. (467 U.S. 986 (1984)) In this case Monsanto requested confidentiality on insecticide information submitted to EPA. There was no doubt that this was trade secret information & could cause competitive harm. Supreme Court ruled that because of the public concern, Monsanto should have known that the data may not remain confidential.

"As long as [Monsanto] is aware of the conditions under which the data are submitted, and the conditions are rationally related to a legitimate Government interest, a voluntary submission of data in exchange for the economic advantages of a registration can hardly be called a taking." (Registration was "voluntary" in that Monsanto didn't have to register unless it wanted to sell its products in the U.S.)

5. Claim of Anti Competitive Implications of Publishing Generator Run Status:
   Arguments of the opponents to disclosure fail to establish any grounds for their claim that disclosure of generator run status information is anticompetitive. They allude to situations where preferential access to such information would be anticompetitive, but those situations have obvious anticompetitive implications. Public disclosure avoids this conflict by ensuring that all commercial interests have broad market visibility and conduct their affairs accordingly. That disclosure may limit the ability of merchants to extract high rents from the market should not imply that disclosure is anticompetitive.
6. "The Real Reason for Disclosure":
   In this paragraph, the opponents of disclosure admit the existence of market power and the potential for its abuse ("You must believe that situations exist in which there are not enough market players to prevent exploitation."). The courts have found in situations absent competition that parties cannot claim substantial harm from disclosure of "confidential" information (*National Parks & Conservation Association v. Morton*, 498 F.2d 765 at p. 770 (D.C. Cir. 1974)). Furthermore, the opponents seek to conceal the existence of such situations from regulators, government agencies and the public.

Memorandum

Peter Steitz, P.E.
Vice President, Power Supply and
Operations
Wisconsin Public Power Inc.
1425 Corporate Center Drive
Sun Prairie, WI 53590
(608) 834-4552
(608) 837-0274 -- FAX
psteitz@wppisys.org

The following statement is submitted in support of the paper entitled: "Generator Run Status: Position Paper Supporting Data Disclosure to the Market Within OASIS Phase II."

This statement is being submitted on behalf of Wisconsin Public Power Inc. (WPPI).

Reasons for Supporting Disclosure

WPPI supports the position paper supporting disclosure of generator run status data within OASIS Phase II for the following reasons:

1. In order to function efficiently, markets need current and accurate information about what is happening with supply and demand. Uncertainty about the supply and demand situation leads market participants to perceive a higher level of risk and to take actions that are not consistent with actions they would have taken with better market information. It is hard to think of a market with a greater need for timely and accurate supply and demand information than the electric utility industry. If electricity market participants are to price their products and commit their resources in a way that will promote the reliability of the electric system and minimize cost, they need accurate and timely information about the demand and supply situation, and generation run status constitutes the key component of the supply-side of the equation.

   The opponents of data disclosure (Position Paper Opposing Disclosure of Generator Run Status Within OASIS Phase II) believe that generator run status information needs to be kept confidential in order to protect the commercial interests of the owners of the generation facilities. Their position, in effect, is that it is more important to enable generating owners to maximize profits than it is to facilitate efficient and reliable electricity markets. We believe that such a shortsighted view, if adopted as a practice within the industry, works ultimately to the disadvantage and harm of all market participants, including the very generators who are seeking to avoid the disclosure of such information.

   In the rapidly disappearing world of the vertically-integrated power system, the control area utility committed and dispatched its resources to meet the real-time and forecasted demand. There was little uncertainty about the supply and demand balance. Now, in the deregulated world of multiple market participants, it is expected by the proponents of non-disclosure that the

multiple suppliers who are aware only of their own generation status will price and dispatch their resources in a way that will provide comparable reliability and lower energy costs than was achieved under the vertically-integrated model. We submit that this will not be possible, if it is indeed possible, without access to supply status (e.g. generator run status) information.

2. Lack of access to information about the supply and demand situation will inevitably create inefficiencies in the market place and reduce reliability. Disclosure of generator run status information is important because it enables all market participants to have a better understanding of actual conditions and to respond accordingly. If certain generators are out of service or not operating, and if this information is restricted only to the owners or purchasers of power from that generation, then the market-participating entities having knowledge of the availability or operational status of that generation will have an advantage over other market participants. The market participants not armed with this knowledge will make less informed decisions than the entities having this knowledge. The uninformed market participants are likely to either over or under commit their generation resources and to over or under-price their energy as a reflection of their lack of knowledge. On average, the pricing decisions of the uninformed participants will be adjusted upward to reflect the uncertainty they perceive about the status of the generation in the market place. If they knew that certain generation is out of service, they may be able to take actions to commit or procure additional resources thereby helping to keep costs lower and maintain reliability. By having to make resource decisions without knowledge of generator run status, the decision making of all market participants will be subject to more guesswork and error than would be the case if they had access to information on generator run status. Thus, the uncertainty created by the lack of access to generator run status information will reduce reliability and contribute to the inefficiency of the market, ultimately translating into higher costs and reduced reliability for consumers.

3. The argument is made by the proponents of non-disclosure that entities whose generators are not available to operate could be hurt economically in the market place by the knowledge that the generation is not available. This argument is problematic for several reasons. First, disclosure of generator runs status information would place all market participants on a level playing field in that no one entity would have an advantage over others if all generators were required to disclose run status information. Second, if a generator knew that its run status information was required to be disclosed, it could factor the potential non availability of its generation and the required disclosure into its operational planning and take measures through appropriate risk management strategies (e.g. diversification and hedging) to mitigate any impact of possible high market pricing when its generation is out of service. Certainly, generators with large portfolios of generation would be protected by the diversity of their portfolios.

4. The proponents of non-disclosure also argue that generation represents only a portion of the supply portfolio and that those with a large proportion of their portfolios in generation would be disadvantaged compared to those with portfolios consisting mainly of contractual and financial assets. This argument also has several problems. One is that generators constitute the supply in the market and not contractual or financial assets. In other words, generators provide the production capability and reliability for the electric system and disclosure is needed to provide the appropriate information needed by the electricity markets. Participants feeling that disclosure would expose their generation portfolios can take appropriate measure to diversity and hedge their risks as discussed under paragraph 3 above.

5. Non-disclosure of information does not prevent gaming. Information about generator run status invariably leaks out and gives those closer to the generator (e.g. neighboring utilities, other

owners of multiple unit plants or merchant functions affiliated with a control area operator) an advantage over those market participants without comparable access or connections. Disclosure would put all market participants on a more equal footing.

6. The need for disclosure of generator run status in the electricity industry is greater than the need for disclosure of gas well and storage status in the gas industry. The primary reason is that the electricity industry cannot economically store its product in significant quantities. Thus, there is no buffer between supply and demand. If the market participants are to respond to the demand/supply situation by committing their resources and pricing their products in real time, they need information that is as accurate and timely as possible.

Why Forecast Information Should Also be Disclosed

The position presented in the paper supporting disclosure of generator run status does not go far enough in our view. We believe that all information concerning generator run status that is required to be submitted to an RTO or security coordinator should be disclosed on the OASIS including information concerning planned maintenance schedules. While it is not possible to eliminate the potential for gaming, the market place will be most efficient and able to respond most adequately to changing conditions if data concerning generator run status that is available to RTOs and security coordinators is also available to all market participants. Such disclosure would put all market participants on the same footing, enable the market place to better respond to real-time and near-term market conditions. This should result in lower costs to consumers and improved system reliability.

Conclusion

The uncertainty created from non-disclosure of generation run status would result in higher costs and reduced reliability. The narrow profit maximization motives of individual generating owners should not override the more important goal of achieving efficient and reliable electric energy markets. There is no proof that disclosure would significantly harm generators if all are required to disclose information. On the contrary, it can be argued that over time all market participants will benefit from disclosure. Generators can reduce potential adverse impacts of disclosure with appropriate risk management strategies (e.g. diversification and hedging).

Non-disclosure was not a problem in the old vertically-integrated electric utility industry structure in which the control area utility tightly controlled production to meet real-time and projected demand. In a world in which the market is expected to play a key role in maintaining reliability, non-disclosure of the supply situation to market participants, both real-time and forecast, is a risky and potentially costly way to proceed.

PS1113M

Oregon Public Utility Commission

The Electronic Scheduling Collaborative
NERC

The State of Orergon Public Utility Commission has reviewed the two papers on disclosure of generator run status drafted for the Electric Scheduling Collaborative and has devoted considerable thought to this issue. It is our opinion that generator plant status data should be disclosed. The issue of generator status information is of critical importance to Oregon for a simple reason. In 1999, Oregon enacted SB 1149 that provides, beginning October 1, 2001, consumers over 30 kW in demand, will purchase electric power at market prices, either directly from wholesale suppliers or from "market-price standard offers" provided through the utility. Furthermore, one major Oregon investor-owned utility does not have sufficient generation to supply all of its loads and so depends on market purchases to meet the utility's load requirements. Therefore, Oregon has placed significant reliance on the wholesale market to serve Oregon loads. Clearly such reliance is justified when the market is functioning well. As you are aware, there is considerable debate over whether price spikes and high market prices in the western United States are caused by market imperfections.

A principle role for government agencies is to establish market structure and rules under which markets operate. One rule that we believe will greatly assist the market is to require each generator operator to disclose generator status. This information will improve system reliability, market pricing, and aid in reducing business risk associated with new generation investment decisions. We oppose those advocating nondisclosure of generator status. Such a position is inconsistent with basic economic theory in that perfect information is assumed when discussing a perfectly competitive market. If a competitive market for electricity is desired then all market participants should have access to this data. Many businesses are established simply to gather and communicate information. We are in the "information age." Those opposed to disclosure are simply creating a market barrier in which entrants must devote financial resources in order to discern generator status information through other means. Erecting this barrier would appear to favor current major owners of generation and those with "deep pockets." We should be doing all that is reasonable and prudent to remove barriers to entry and business risks.

We note that while we support disclosure of generator status information, the OPUC is not advocating disclosure of bidding practices or generation cost data. This truly "competitive" information would remain protected. In addition, the OPUC is not recommending disclosure of forecast generation/transmission information.

These issues are critical to Oregon and the western United States. We look forward to further participating in the crafting of market rules and structure that facilitate a vibrant competitive wholesale market. In doing so, all citizens and businesses will be well served and our transition to a new electric industry structure will be well founded.

Ron Eachus	Joan Smith	Roger Hamilton
Chairman	Commissioner	Commissioner

Vanessa Jeffery
Engineer, Supply and Trading
Salt River Project
Phoenix, AZ
vajeffer@srpnet.com

After reviewing both position papers, SRP Merchant does not support disclosing generator-run status on OASIS Phase II.

January 24, 2001
Comments to: Electronic Scheduling Collaborative Position Papers Supporting Data Disclosure to the Market

Submitted by: Vern Colbert
Dominion Virginia Power
vern_colbert@dom.com

The two papers submitted do a good job discussing this very difficult subject and we appreciate the difficulty the ESC has had trying to reach consensus on this. Instead of repeating what has already been said we would simply put forth our position that we are opposed to posting generator run status for two reasons:

- In a perfect world where all participants had equal capabilities we would agree that posting generator run status would simply provide additional information of use to all participants. But we have seen clearly in recent months how imperfect generation markets can be and how those able to process information better than others can use this to their advantage in the spot market. For this reason alone we would be opposed to providing generator run status or any other system data that could produce more distortions in supply or price.

- Even if the data discussed could be provided without the threat of additional distortions to generation supply and price, we are still opposed to this initiative until some leveling-out time is allowed in the industry. The number of separate programs already underway (RTO formations, OASIS II, compliance programs, disaggregation of functions, etc.) simply need to have more time allowed without putting additional requirements on the industry to supply data.

As a final note we would add that if it were desired to post additional data (which we are against), it would be just as easy to post all applicable generator data not just run status, and let users see everything. By doing this we would think that this posting could actually enhance system security by presenting a more whole picture.

Attachment 8

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

OASIS Standards Collaborative Scope

Developed by: OASIS Standards Collaborative (OSC)

Draft

January 7, 2001

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

OASIS Standards Collaborative
Scope

Draft 2-7-2001

Purpose

The OASIS Standards Collaborative (OSC) is a technical collaborative of the Electric Power Industry for developing standards and communications protocols for Open Access Same-Time Information System (OASIS). It works both with, and independently from the Electronic Scheduling Collaborative to develop a cohesive technical approach for implementation of OASIS. OSC will work to resolve technical issues related to OASIS, presented by various NERC groups and the industry.

The group was initially comprised of the members of the NERC Transaction Information Systems Working Group (TISWG) and the OASIS How Working Group to draw on the experience of the TISWG in E-Tags and the OASIS How Working Group in their past work on OASIS and FERC filings.

Activities

The OSC will develop standards and communications protocols for OASIS, in compliance with federal regulations, to enable the market to:

- View information postings
- Procure transmission rights
- Procure ancillary services
- Schedule transmission services and energy
- Audit transactions

The OSC will also have initial responsibility for:

- Identifying and developing Business Practices in conjunction with the Electronic Scheduling Collaborative (ESC) and the NERC Market Interface Committee (MIC).
- Implementation of OASIS 1.4
- Development of E-Tag 1.7
- Development of Standards and Communications Protocols (S&CP) for OASIS Phase II (electronic scheduling)

Task Groups

Separate task groups will be formed to concentrate on specific aspects of OASIS as required. Participation in any task group is open to all industry participants. The following initial task groups have been identified:

- E-Tag Data Modeling and Business Analysis Group
- OASIS Data Modeling and Business Analysis Group (To be merged with E-Tag Data Modeling later)
- Protocol Group (e.g., HTTP, SOAP/SMXP)
- Security Group
- Business Practices Implementation Group

- Standards Development Process Group

Coordination and Liaisons

The OSC will coordinate with and maintain close liaison relationships with the NERC and Industry groups:

- Electronic Scheduling Collaborative (ESC)
- NERC Standing Committees
- Interchange Subcommittee (IS)
- Transaction Information Systems Working Group (TISWG)
- Project Management Team (PMTeam)
- Interchange Distribution Calculator Working Group (IDCWG)
- Control Area Criteria Task Force (CACTF)
- Central Repository Task Force (CRTF)
- All other groups as appropriate

Representation on the OSC

1. Membership in the OSC and participation in the OSC meetings are open to all Utility Industry participants.
2. EPRI and NERC staff coordinator support.

Governance

1. Roberts Rules of Order, as implemented by NERC, will be employed.
2. All OSC industry participants have voting rights.
3. Chair and Vice Chair have voting rights.
4. Motions carry upon receipt of affirmative votes exceeding two-thirds of the total votes (including abstentions) cast.
5. Non voting members are EPRI and NERC staff coordinator(s).
6. Chair and Vice Chair – initially appointed by the Chair of the Electronic Scheduling Collaborative. Future Chair and Vice Chair will be selected from active membership. The length of the appointment will be one year.
7. For voting there must be a quorum of at least 9 voting members.
8. Multiple representatives from a given company or organization are limited to a single vote unless they clearly represent different industry segments (e.g., Transmission Provider vs. Merchant Affiliate).

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Simple Method eXchange Protocol (SMXP) and Style Guide 1.0

Developed by: OASIS Standards Collaborative (OSC)

Draft

January 6, 2001

INTENTIONALLY
BLANK

Table of Contents

Table of Contents 3
1 Introduction 5
1.1 Scope 5
1.2 Overview 5
1.3 XML Schema Notation 6
1.4 Notation Convention 6
1.5 Example SMXP Message 6
2 Message Exchange Model 7
3 SMXP Message Framework 7
3.1 Envelope 7
3.2 Header 7
3.3 Body 8
3.4 Fault 8
3.4.1 Fault Codes 9
4 Encoding 10
4.1 Terminology 10
4.2 Serialization Rules 12
4.2.1 Structures (struct) 12
4.2.2 Arrays 12
4.3 Unknown or Null values 13
4.4 Default values 14
4.5 Date and Time data 14
5 XML Conventions 14
6 HTTP 15
6.1 HTTP URL 15
6.2 HTTP Example 16
7 Security 16
7.1 HTTP Basic Authentication 16
7.2 SSLv3.0 and TLS1.0 17
7.3 Authorization 19
8 Method Encoding 19
8.1 Headers 19
8.2 Request/Calls 19

8.3 Response/Reply ____ **20**
8.4 Get Method Parameters ____ **20**
8.5 Set Method Parameters ____ **21**
8.6 New Method Parameters ____ **21**
8.7 Other Methods ____ **21**
9 Method XML-Schema conventions ____ ***22***
10 Method Examples ____ ***22***

1. Introduction

The **S**imple **M**ethod e**X**change **P**rotocol (SMXP) is an XML based protocol designed for use via HTTP. It implements a simple RPC style of request/reply messaging utilizing the Simple Object Access Protocol (SOAP) framework as a basis. The protocol is intended as a very simple, open and flexible mechanism for creating interfaces across disparate programming languages and operating systems. Whenever possible, the simplest form of the SOAP framework has been chosen.

1.1 Scope

This document describes the Simple Method Exchange Protocol (SMXP) and numerous style guidelines and rules. It is intended for use by those systems or individuals that are:

Implementing SMXP
Making SMXAPI calls against a system that supports SMXP.
Implementing and defining SMXAPI interfaces that must comply with the SMXP

This document is intended to be used in conjunction with the SOAP 1.1 specification located at http://www.w3.org/TR/SOAP and the October 24,2000, W3C XML Schemaa Candidate Recommendation located at http://www.w3.org/TR/xmlschema-0/. However, the SOAP 1.1 specification should be used as a reference only and this document shall take precedence.

1.2 Overview

The SMXP makes use of the SOAP 1.1 messaging framework as described in the W3C note dated May 08, 2000 and located at http://www.w3.org/TR/SOAP/. SMXP and the SMXAPI do not, however, attempt to make complete use of the XML-SOAP message encoding as described in section 5 of the standard reference above. Instead, the SMXP uses a simple encoding style that is similar to SOAP's and that this document will describe. The encoding style described is the basis of SMXAPI interfaces and methods.

SMXP implements the HTTP POST binding as described in section 6 of the SOAP specification and will NOT utilize the HTTP extensions option. However, it would be possible to implement SMXP using SMTP with little or no modification as a request/reply style of message exchange is used. However, unless stated otherwise, HTTP is the assumed and preferred transport.

SMXP does not require the complete support of SOAP or all of its options, but rather, a subset of its features are implemented and used as a framework for implementing SMXAPI interfaces. SMXP is, however, FULLY compliant with the SOAP 1.1 specification and implements all REQUIRED, MUST, and SHALL components of the specification. Specifically, sections 1, 2, 3, 4, 6, and 7 are applicable to SMXP and should be referenced for additional information. Any restrictions, or variations from the SOAP 1.1 standard, will be noted in this document. Some of the information contained within the SOAP 1.1 specification will be repeated within this document for completeness and clarification.

1.3 XML Schema Notation

Unless otherwise noted, all XML Schemas will be created and reference using the XML-Schema standard as defined by the W3. SOAP uses XML-Schema as its meta-language and SMXP adopts this standard in turn.

1.4 Notation Convention

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.
Within this document, namespace URIs of the general form "some-URI" represent some application-dependent or context-dependent URI.
Within this document, namespace URIs of the general form “method-URI” represent some method/interface-dependant or context-dependent URI.

1.5 Example SMXP Message

The example below shows a simple example SMXP message.

HTTP SMXP Request Message:

```
POST /GenericApplication/SomeProgram HTTP/1.0
Host: www.somenode.com
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: “GenericApplication:GetMethod”

<Envelope>
  <Header>
     <h:Transaction xmlns:h=”method-URI”>
          3X112
     </h:Transaction>
   </Header>
   <Body>
       <GetMethod xmlns=”method-URI”>
          <Parameter1>
               <Item>Some Value</Item>
                    *
                    *
                    *
          </Parameter1>
          <Parameter2>###</Parameter2>
      </GetMethod>
    </Body>
</Envelope>
```

The HTTP reply:

```
HTTP/1.0 200 OK
Content-Type: text/xml; charset="utf-8"
```

```
Content-Length: nnnn

<Envelope>
  <Header>
     <Transaction xmlns=”http://xml-smxp.com/smxp/common/”>
          3X112
     </Transaction>
   </Header>
   <Body>
       <GetMethodResponse xmlns=”method-URI”>
           <GetMethodReturn>
                <Item>Some Value</Item>
                    *
                    *
                    *
            </GetMethodReturn>
        </GetMethodResponse>
   </Body>
</Envelope>
```

2. Message Exchange Model

SMXP messages are implement using the request/response pattern over HTTP. Other patterns are NOT supported using SMXP at this time. Refer to section 2 of the SOAP specification for more information.

3. SMXP Message Framework

The SMXP, as with SOAP, contains an Envelope element, a Header element, a Body element, and a Fault element (if necessary). The simplest allowable form of these elements has been chosen from the SOAP specification. Specifically, a default namespace is applied or assumed for the Envelope element thus eliminating the requirement to qualify every SOAP element explicitly (i.e., SOEP-ENV:Header)

3.1 Envelope

- The element name is "Envelope".
- The element MUST be present in an SMXP message
- The element MAY contain a default namespace of xmlns=”http://schemas.xmlsoap.org/soap/envelope/”. If not specified, it MUST be assumed.

3.2 Header

- The element name is " Header".
- The element MUST be present in a message, even if no Header entries are made, and MUST be the first immediate child element of an Envelope element.
- Any children elements (Header entries) must be namespace qualified. The preferred method is to apply a default namespace to each header entry as in <HeaderEntry xmlns=”some-URI”>

- The element MAY contain the <Transaction xmlns="http://xml-smxp/smxp/common/" [TWK2]header entry. The Transaction element, if used, MUST be an immediate child element of the Header element and MUST be SMXP namespace-qualified. The Transaction header entry is set by the calling application and MUST be returned in the response message header unchanged. Its value can be any string that the calling application wishes to set.
- A reply/response MAY contain the <Warning xmlns="http://xml-smxp/smxp/common/" header element. If included in the response, it MUST be the first child element of the Header element. It's contents are free-form and at the discretion of the method implementer. However, its use should be associated with non-critical errors such as the use of a deprecated interface.
- MUST contain any Header elements described in an SMXAPI Method Schema (see section ?). Example might include <MaxRecords/> or <RecordsReturned> and may be different for both the request and reply.
- All header entries MUST be namespace qualified.

3.3 Body

- The element name is "Body".
- The element MUST be present in SMXP messages and MUST be an immediate child element of a SOAP Envelope element and it MUST directly follow the SOAP Header element.
- The element contains a set of body entries each being an immediate child element of the SOAP Body element that follow the method encoding scheme detailed below and in the SOAP 1.1 specification. SOAP defines the SOAP Fault element, which is used to indicate error messages (see section 4.4). The Fault mechanisms associated with SMXP will be described in further detail below.

3.4 Fault

- The SOAP Fault element is used to carry error and/or status information within an SMXP message. If present, the SOAP Fault element MUST appear as a body entry and MUST NOT appear more than once within a Body element.
- The SOAP Fault element defines the following four subelements, but only faultcode, faultstring and detail will typically be used in SMXP. The use of faultactor and detail will be up to the discretion of each method implementation:
- faultcode
- The faultcode element is intended for use by software to provide an algorithmic mechanism for identifying the fault. The faultcode MUST be present in a SOAP Fault element and the faultcode value MUST be a qualified name as defined in [8], section 3. SOAP defines a small set of SOAP fault codes covering basic SOAP faults (see section 4.4.1)
- faultstring
- The faultstring element is intended to provide a human readable SMXPlanation of the fault and is not intended for algorithmic processing. The faultstring element is similar to the 'Reason-Phrase' defined by HTTP (see [5], section 6.1). It MUST be present in a SOAP Fault element and SHOULD provide at least some information describing the nature of the fault.
- faultactor (OPTIONAL)
- The faultactor element is intended to provide information about who caused the fault to happen within the message path (see section 2). It is similar to the SOAP actor attribute (see section 4.2.2) but instead of indicating the destination of the header entry, it indicates the

source of the fault. The value of the faultactor attribute is a URI identifying the source. Applications that do not act as the ultimate destination of the SOAP message MUST include the faultactor element in a SOAP Fault element. The ultimate destination of a message MAY use the faultactor element to indicate explicitly that it generated the fault (see also the detail element below).

- detail (OPTIONAL) The detail element is intended for carrying application specific error information related to the Body element. It MUST NOT be used to carry information about error information belonging to header entries. Detailed error information belonging to header entries MUST be carried within header entries. All immediate child elements of the detail element are called detail entries and each detail entry is encoded as an independent element within the detail element.

3.4.1 Fault Codes

- The faultcode values defined in this section MUST be used in the faultcode element when describing faults defined by this specification. The namespace identifier for these faultcode values is "http://schemas.xmlsoap.org/soap/envelope/". Use of this space is recommended (but not required) in the specification of methods defined outside of the present specification.
- The default SOAP faultcode values are defined in an extensible manner that allows for new SOAP faultcode values to be defined while maintaining backwards compatibility with existing faultcode values. The mechanism used is very similar to the 1xx, 2xx, 3xx etc basic status classes classes defined in HTTP (see [5] section 10). However, instead of integers, they are defined as XML qualified names (see [8] section 3). The character "." (dot) is used as a separator of faultcode values indicating that what is to the left of the dot is a more generic fault code value than the value to the right. Example

```
Client.Authentication
```

- The set of faultcode values defined in this document is:

Name	Meaning
VersionMismatch	The processing party found an invalid namespace for the SOAP Envelope element (see section 4.1.2)
MustUnderstand	An immediate child element of the SOAP Header element that was either not understood or not obeyed by the processing party contained a SOAP mustUnderstand attribute with a value of "1" (see section 4.2.3)
Client	The Client class of errors indicate that the message was incorrectly formed or did not contain the appropriate information in order to succeed. For example, the message could lack the proper authentication or payment information. It is generally an indication that the message should not be resent without change. See also section 4.4 for a description of the SOAP Fault detail sub-element.
Server	The Server class of errors indicate that the message could not be processed for reasons not directly attributable to the contents of the message itself but rather to the processing of the message. For

	example, processing could include communicating with an upstream processor, which didn't respond. The message may succeed at a later point in time. See also section 4.4 for a description of the SOAP Fault detail sub-element.

4. Encoding

SMXP encoding style follows the general SOAP form but does NOT attempt strict conformance with SOAP encoding.

4.1 Terminology

1. To describe SMXP encoding, the following is used:
2. A "value" is a string, the name of a measurement (number, date, enumeration, etc.) or a composite of several such primitive values. All values are of specific types.
3. A "simple value" is one without named parts. Examples of simple values are particular strings, integers, enumerated values etc.
4. A "compound value" is an aggregate of relations to other values. Examples of Compound Values are particular purchase orders, stock reports, street addresses, etc.
5. Within a compound value, each related value is potentially distinguished by a role name, ordinal or both. This is called its "accessor." Examples of compound values include particular Purchase Orders, Stock Reports etc. Arrays are also compound values. It is possible to have compound values with several accessors each named the same.
6. An "array" is a compound value in which ordinal position serves as the only distinction among member values.
7. A "struct" is a compound value in which accessor name is the only distinction among member values, and no accessor has the same name as any other.
8. A "simple type" is a class of simple values. Examples of simple types are the classes called "string," "integer," enumeration classes, etc. SMXP adopts all the types found in the section "Built-in datatypes" of the "XML Schema Part 2: Datatypes" Specification [11], both the value and lexical spaces.
9. A "compound type" is a class of compound values. An example of a compound type is the class of purchase order values sharing the same accessors (shipTo, totalCost, etc.) though with potentially different values (and perhaps further constrained by limits on certain values).
10. Within a compound type, if an accessor has a name that is distinct within that type but is not distinct with respect to other types, that is, the name plus the type together are needed to make a unique identification, the name is called "locally scoped." If however the name is based in part on a Uniform Resource Identifier, directly or indirectly, such that the name alone is sufficient to uniquely identify the accessor irrespective of the type within which it appears, the name is called "universally scoped."
11. If only one accessor can reference it, a value is considered "single-reference". If referenced by more than one, actually or potentially, it is "multi-reference." Note that it is possible for a certain value to be considered "single-reference" relative to one schema and "multi-reference" relative to another. (** SMXP SHALL NOT allow multi-referenced values)

12. Syntactically, an element may be "independent" or "embedded." An independent element is any element appearing at the top level of a serialization. All others are embedded elements.

4.2 Serialization Rules

General rules for serialization are as follows:

1. All values are represented as element content. Multi-reference value SHALL NOT be used. (**)
2. For each element containing a value, the type of the value MUST be represented by the name of the element bearing a definite relation to the type and that type then determinable from a schema. (**)
3. A simple value is represented as character data, that is, without any subelements. Every simple value must have a type that is either listed in the XML Schemas Specification, part 2 [11] or whose source type is listed therein (see also section 5.2).
4. A Compound Value is encoded as a sequence of elements, each accessor represented by an embedded element whose name corresponds to the name of the accessor. Accessors whose names are local to their containing types have unqualified element names; all others have qualified names (see also section 5.4).

(**) deviation from the SOAP1.1 serialization rules.

4.2.1 Structures (struct)

As previously defined, a "struct" is a compound value in which accessor name is the only distinction among member values, and no accessor has the same name as any other. The XML-Schema used to define a structure SHALL be modeled as a sequence of elements and follow the following convention and form:

```
     <element name = "Structure">
          <complexType content = "elementOnly">
               <sequence>
                    <element ref = "Accessor1"/>
                    <element ref = "Accessor2"/>
                    <element name=”Accessor3” type=”date”/>
                                             <element ref =
"Accessor4"/>
               </sequence>
          </complexType>
     </element>

     <element name = "Accessor1" type = "int"/>
     <element name = "Accessor2" type = "string"/>
     <element name = "Accessor4" type = "Array"/>
```

The accessor elements may reference other elements, simpleTypes or other compound types. Each accessor of a struct SHALL only be allowed to appear once and MUST have unique names. Any compound element that follows the convention above SHALL be assumed to be a struct.

4.2.2 Arrays

As previously defined, an "array" is a compound value in which ordinal position serves as the only distinction among member values. Each element in an array must be of the same type and

name and may appear multiple times. Accessor elements may reference another element, simple types, or other compound types (like other structs or arrays). The XML-Schema used to define an array SHALL be modeled as a sequence of same-type elements, or a sequence of identically named elements (via a reference), and follow the following general convention and form:

```
     <element name = "Array">
          <complexType content = "elementOnly">
               <sequence>

                    <element name = "Element2" ref="Element1"

minOccurs = "1" maxOccurs = "unbounded"/>

               </sequence>
          </complexType>
     </element>


     <element name = "Element1" type = "string"/>
     <element name = "Element3" type = "Element1"/>
```

Any element that follows these conventions SHALL be assumed an array.

4.3 Unknown or Null values

If the absence of a data value or an undefined state is important to convey in either a request or replay, the standard XML-Schema practice of coding an empty element and using the “null” attribute will be used.

XML Schema's null mechanism involves an "out of band" null signal. In other words, there is no actual null value that appears as element content, instead there is an attribute to indicate that the element content is null. To illustrate, we can modify the shipDate element declaration so that nulls can be signalled:

```
<xsd:element name="shipDate" type="date" nullable="true"/>
```

And to explicitly represent that shipDate has a null value in the instance document, we set the null attribute (from the XML Schema namespace for instances) to true:

```
<shipDate xsi:null="true"></shipDate>
```

The null attribute is defined as part of the XML Schema namespace for instances (http://www.w3.org/1999/XMLSchema-instance), and so it must appear in the instance document with a prefix (xsi:) associated with that namespace. (As with the xsd: prefix, the xsi: prefix is used by convention only). Note that the null mechanism applies only to element values, and not to attribute values. An element with xsi:null="true" may not have any element content but it may still carry attributes.

The default, if not explicitly specified in the XML Schema, is that nullabe=”true” and xsi:null=”false”. If an element was defined as:

```
<xsd:element name="Comment" type="string" nullable="true"/>

The following cases would be interpreted as follows:

<Comment></Comment> is known to be an empty string; and
<Comment xsi:null=”true”></Comment> is set to null or unknown
```

4.4 Default values

An omitted accessor element implies a default value if specified in the XML Schema or null or unknown if a default is not specified and nullable=”yes”; if nullable=”false” and minOccurs is > 0, then it is an error. The specifics depend on the accessor, method, and its context. It should be noted, however, that XML-Schema does not currently have a mechanism for defining default values of elements and an additional attribute or notation would be required.

4.5 Date and Time data

XML-Schema defines many Simple Types relating to dates and time. Those types, and their associated notations, follow the ISO 8601 standard and SHALL be used to represent dates and times in any SMXP methods. Of particular use is the “timeInstant” dataType that includes an offset from GMT. An example is:

```
1999-05-31T13:20:00.000-05.00
```

Which stands for “May 31st 1999 at 1:20PM Eastern Standard Time (which is 5 hours behind coordinated universal time.

It is acceptable to omit the hyphens and colons in the above example. This is called the “basic format” as apposed to the “extended format.” To represent a value in GMT (UTC), a trailing “Z” shall be appended without spaces as shown in the example below:

```
1999-05-31T13:20:00.000Z or
19990531T132000000Z
```

When the application clearly identifies the need for an expression of only date and time of day, milliseconds may be omitted. Refer to the XML-Schema for a method for specific format requirements.

Unless a specific need exists, the “basic format” shall be the preferred format and specified in GMT, as in **“19990531T132000000Z.”**

5. XML Conventions

All XML-Schemas (Elements and Attributes) should follow these general conventions:

1. All elements MUST have their first letter upper case with each subsequent word, phrase, or acronym capitalized. This convention is known as UpperCamelCase.

2. All attributes MUST have their first letter in lower case with each subsequent word, phrase, or acronym capitalized. This convention is known as lowerCamelCase.
3. The use of special characters, such as underscored and hyphens, SHOULD be avoided in element and attribute naming.
4. Enumerations (allowable values) for attributes will follow the same naming standard as attributes.
5. All data values are represented as element content.
6. Attributes shall only be used to describe behavior or further qualify or describe a data value represented as element content.

6. HTTP

SMXP does not employ the HTTP extension mechanism described in the SOAP specification (**). SMXP does, however, REQUIRE the use of the SOAPAction HTTP header field. The SOAPAction HTTP request header field can be used to indicate the intent of the HTTP request. The value is a URI identifying the intent. SOAP places no restrictions on the format or specificity of the URI or that it is resolvable. An HTTP client MUST use this header field when issuing a SOAP HTTP Request, even if it is left empty.

```
soapaction  = "SOAPAction" ":" [ <"> URI-reference <"> ]
URI-reference = <as defined in RFC 2396 [4]>
```

The presence and content of the SOAPAction header field can be used by servers, such as firewalls, to appropriately filter SOAP request messages in HTTP. The header field value of empty string ("") means that the intent of the SOAP message is provided by the HTTP Request-URI. No value means that there is no indication of the intent of the message.

Examples:

```
SOAPAction: "http://electrocommerce.org/abc#MyMessage"
SOAPAction: "myapp.sdl"
SOAPAction: ""
SOAPAction:
```

The SMXP preferred value of the SOAPAction HTTP header field is a URI composed of the API or application name + “:” + MethodName. If a method was called “GetStockQuote” and it was in the set of methods from the QuoteServer application, the entry would be:

```
SOAPAction: “QuoteServer:GetSTockQuote”
```

It is acceptable, however, to leave the field blank if the context of the SOAPAction can be derived from the POST HTTP Header entry.

6.1 HTTP URL

The URL of the POST is up to the method implementer or shall be documented in the method’s schema by the method author.

6.2 HTTP Example

HTTP Using POST

```
POST /GetStockQuote HTTP/1.1
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "QuoteServer:GetStockQuote”

<Envelope...

HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn

<Envelope...
```

7. Security

SMXP messages may be secured using HTTP Basic Authentication, Secure Sockets Layer, version 3.0, (SSLv3.0), or using Transport Layer Security, version 1.0 (TLSv1.0). The difference between the SSLv3.0 and TLSv1.0 specifications is rather minor, but SSLv3 is much better known than TLSv1.0 and more widely implemented. However, if an application or system is capable of supporting TLSv1.0, it should be considered (See RFC 2246/2818 for TLSv1.0 specification). Most implementations of TLSv1.0 provide backward compatibility with SSLv3.

7.1 HTTP Basic Authentication

HTTP Basic Authentication may be used to provide a rudimentary form of username/password client authentication. It is not a form of strong authentication and does not provide for mutual authentication (both client and server), encryption, message integrity, or non-repudiation services. If any of those security features are required, SSLv3.0 or TLSv1.0 must be used.

HTTP Basic Authentication is described in RFC 1945 and 2065 as it relates to HTTP 1.0 and 1.1 respectively. To employ HTTP Basic Authentication, the HTTP Authorization header is sent to the server by the client in the general form:

Authorization: Basic username:password

Where the username:password is Base 64 encoded. For the username of webmaster and the password of zrqma4v, the Authorization header would look like:

Authorization: Basic d2VibWFzdGVy0npycW1hNHY=

If a client attempts to access a server resource that is secured using HTTP Basic Authentication, the server shall return an HTTP error code of 401 and the HTTP header:

WWW-Autheticate: Basic realm=”WallyWorld”

where "WallyWorld" is a string assigned by the server to identify the protection space of the Request-URI.

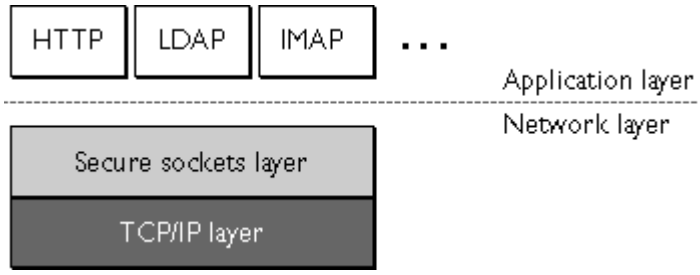
Base 64 encoding and decoding is a very easy function to implement. As such, an intercepted message between a client and a server that is employing Basic Authentication could have its username and password easily compromised.

7.2 SSLv3.0 and TLS1.0

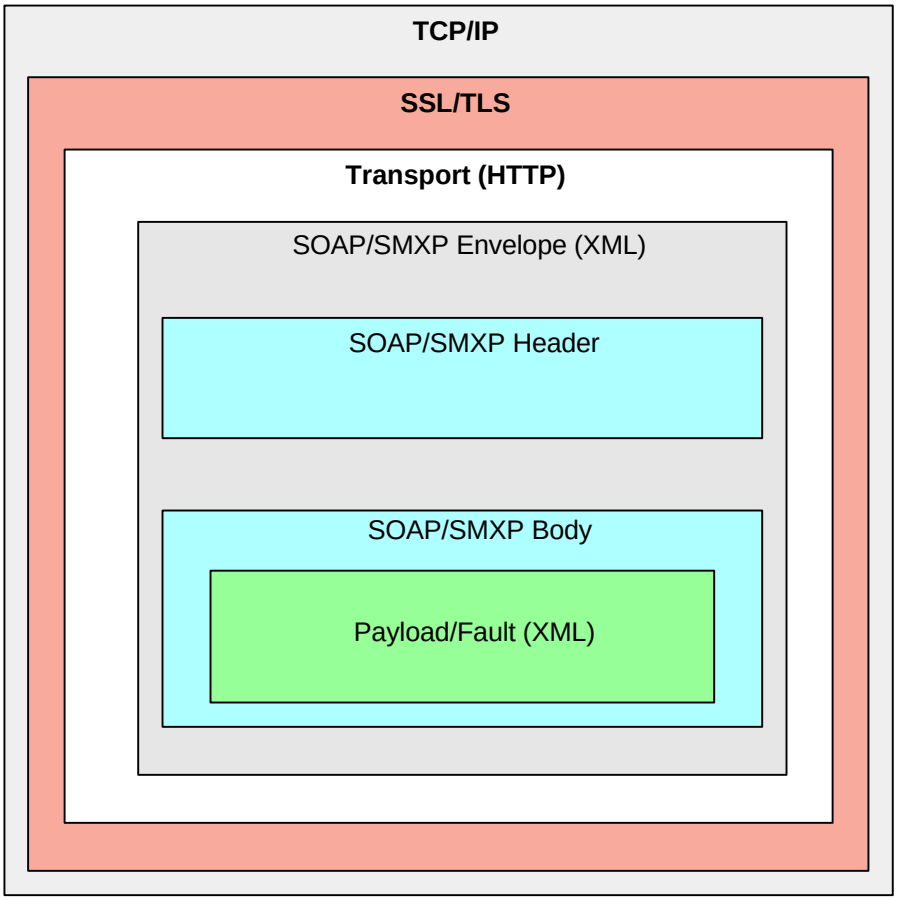
When employing SSLv3.0 or TLSv1.0 to secure an SMXP message or session, only X.509, version 3, certificates shall be used (X.509v3). Older certificate formats shall not be accepted by either party (client or server).

The SSL/TLS protocols run above TCP/IP and below higher-level protocols such as HTTP, LDAP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows: an SSL-enabled server to authenticate itself to an SSL-enabled client; the client to authenticate itself to the server; and both machines to establish an encrypted connection.

Both SSL and TLS are considered separate security protocol layers as shown in the diagram below.



When used to secure an SMXP message over http, the resulting message can be depicted as in the diagram below.



It is beyond the scope of this document to further describe SSL or TLS. Many open source and commercial libraries exist and may be used to secure SMXP messages. Specific security requirement must be evaluated by each application/system to determine if both client and server authentication is required (mutual authentication), certificate key lengths (512/1024/2048), encryption key lengths (40/128), and any other specific Certificate Policies that may need to be enforced (smart cards, etc.).

When employing SSLv3.0, some standard HTTP error codes that should be returned to a client include:

HTTP error	
Error code	**Cause**
403.4	SSL Required
403.5	SSL 128 Required
403.7	Client Certificate Required

7.3 Authorization

The authorization scheme employed to determine the rights, priviledges, and resources that a client may access (i.e., methods that may be invoked), is beyond the scope of this document and SMXP. Each application, system, or environment should determine its own authorization rules.

8. Method Encoding

All SMXP methods referenced together as part of an application or system are called an SMXAPI. An SMXAPI method MUST be described in an XML-Schema and contain a method element, a response element, and MAY contain Header elements. The XML-Schema describing an SMXAPI method must also be scoped within a namespace.

An application processing a method MAY process requests with missing parameters if they are optional in the XML-Schema description of the method. However, this is not the preferred form and if possible, all method parameters SHOULD be present.

Because a result indicates success and a fault indicates failure, it is an error for the method response to contain both a result and a fault.

SMXAPI method's call and response are both carried in the SOAP Body element (see section 4.3) using the following representation:

8.1 Headers

In addition to the standard SMXP <Transaction> and <Warning> header elements, each SMXP method may define additional header entries in the XML-Schema that described the method. These methods SHOULD be scoped within the same namespace as the method itself. Method headers may be different for the request and response and sufficient comments MUST be provided within the schema to describe their use and function.

8.2 Request/Calls

1. SMXAPI methods requests (and responses) MUST be modeled as a single structure (see earlier description of structures) element containing an accessor for each [in] or [in/out] parameter. The struct is both named and typed identically to the method name.
2. Method names SHOULD follow a "Get" and "Set" and "New" or Verb/Noun paradigm and an UpperCamelCase convention where the first letter is upper case and each subsequent word or phrase's first letter is upper case. An example is "GetScheduleDetail" or "SetMeterLevel". If a "Get/Set/New" paradigm isn't appropriate, a "VerbNoun" convention is preferred for all alternate naming of Methods
3. Each parameter accessor has a name corresponding to the name of the parameter and type or reference corresponding to the type of the parameter.
4. Method element MUST be default namespace qualified in the same namespace as the XML-Schema method description. Each first-level child element (accessor) contained within the method element MUST have a unique name and be non-repeating.
5. Each accessor element is viewed as a method parameter, with a name corresponding to the name of the parameter and type or reference corresponding to the type of the

parameter. These appear in the same order as in the method signature and MAY be optional.

6. Method elements MAY contain attributes of simpleTypes as described in the XML-Schema Datatypes specification. It may also contain the “unique” attribute (see section 8.5).
7. These attributes SHALL NOT be considered parameters to the method and shall only be used to specify behavior or further qualify the data value contained within the element.
8. Parameters MAY contain children elements or other complexType constructs.
9. Parameter elements MAY also contain attributes, in addition to the standard SMXP encoding attributes of “function” and “operator” (described below)
10. For repeating data, such as a capacity profile, the repeating data SHOULD be modeled as an array as described above (4.2.2). A naming convention of appending an “s” or “List” or “Profile” is recommended.

8.3 Response/Reply

1. The reply/response element name MUST be the method name with the string "Response" appended. Responses MUST be modeled as a single structure element (see earlier description) containing an accessor for each [return], [out] or [in/out] parameter.
2. The first accessor MUST be the [return] value followed by the [out] and [in/out] parameters in the exact same order as in the method signature.
3. For the return value accessor name, append after the method name the string “Return” (e.g., MethodReturn)
4. Regardless of whether the SMXAPI method has a return value, a return value accessor MUST be present in the reply. If no return value is necessary, an empty element MAY be used (<MethodReturn/>)
5. A method fault is encoded using the SOAP Fault element (see section 3.4) and its use will be described below.

8.4 Get Method Parameters

- Method element accessors will constitute the query parameters.
- Accessors SHALL be and-ed together unless the “function" attribute indicates otherwise. Allowable functions are “and” and “or” and MUST always be presumed to be with respect to the previous accessor/parameter. The method’s XML-Schema MUST specify the allowable functions and a default if other than “and.”

```
<GetMethod xmlns=”method-URI” >
     <Parameter1>#####</Parameter1>
     <Parameter2 function=”or”>#####</Parameter2>
          *
</GetMethod>
```

- Accessor values SHALL be assumed to be equality (=) unless the “operator” attribute indicates otherwise. Allowable operators are “=”, “>”, “<”, “>=”,”<=”, and the “not” form by using a “!” as the first character of the action (i.e,. “!=”). The method’s XML-Schema MUST specify the allowable actions and default if other than “=.”

```
<GetMethod xmlns=”method-URI” >
```

```
   <Parameter1>#####</Parameter1>
   <Parameter2 function=”or” operator=”>”>####</Parameter2>
          *
</GetMethod>
```

- When the accessor/parameter is an array of elements, the function attribute MAY be set on the array as an attribute of the array. The default function is “and” if not specified. All the elements within the array are grouped together for purposes of query evaluation. Elements of the array may have the function or operator attributes defined on them as allowed for in the methods Schema and will relate only to within the scope of the array. (See examples.) The default function and operator for elements within the array (array accessors) shall be “or” and “=”. If the first element of an array has the “function” attribute applied to it, it shall be ignored.
- Get methods MAY return structs or arrarys of elements.
- As a convention, array names SHOULD be the name of the element/type contained within the array with an “s” or “List” or “Profile” appended to the end.

8.5 Set Method Parameters

- Set methods will be composed of two types of accessors. The first type define the records (or objects/instances) to be updated and follow the rules of the Get accessors and are equivalent to a “where” clause in SQL or identify some type of unique identifier. The second type contains the actual data to be “set”. The where parameters MUST be first, followed by the data parameters.
- An attribute of the method element called “unique” can be set to “yes” or “no” depending on if the data to be updated should only be one record/object or can be multiple records/object. The default is “yes” and would require the method to refer to exactly one record/object/instance. The method implementer does NOT have to support multi-record/object updates and can declare the option in the method’s Schema.

```
<SetMethod xmlns=”method-URI” unique=”no” >
          *
          *
</SetMethod>
```

8.6 New Method Parameters

- A “New” method is responsible for creating new records/objects/instances. The parameters defined in the methods XML-Schema define the new record/object/instance in sufficient detail as to allow the method implementer to create it.
- The “unique”, “function” and “operator” attributes, even if defined in the XML-Schema and specified in the method request, MUST be ignored.

8.7 Other Methods

Method types other than Get, Set, and New may be defines as needed and may follow a different naming scheme, such as VerbNoun. Such methods will typically embody a high level function. Examples might include:

CurtailSchedule
BillCustomer
RemoveOffer

9. Method XML-Schema conventions

The XML-Schema used to describe a method should contain sufficient comments to convey any special behavior, restrictions, or assumptions. Specific documentation standards and conventions will be determined at a later date (TBD).

10. Method Examples

Method Example (without HTTP or schema shown):

Schedules[] **GetSchedule**(POR[] PORlist, POD[] PODlist, FromCA[]FromCAlist, ToCA[] ToCAlist, Customer[] Customerlist, Agreement[] Agreements, Reservation[] Reservations, dateTime StartTime, dateTime StopTime,
dateTime TimeOfLastUpdate)

```
<?xml version ="1.0"?>
<GetSchedule>
     <BeginFlow function = "and" operator =
"&lt;=">20000407T183909Z</BeginFlow>
     <EndFlow function = "and" operator =
"&gt;=">20000307T183909Z</EndFlow>
     <StatusList function = "and">
          <Status function = "or" operator =
"=">Scheduled</Status>
     </StatusList>
     <UPCAList function = "string">
          <UPCA function = "or" operator = "=">AVA</UPCA>
          <UPCA function = "or" operator = "=">BCHA</UPCA>
          <UPCA function = "or" operator = "=">SCL</UPCA>
     </UPCAList>
     <DNCAList function = "string">
          <DNCA function = "or" operator = "=">CISO</DNCA>
          <DNCA function = "or" operator = "=">LDWP</DNCA>
     </DNCAList>
     <PORList function = "string">
          <POR function = "or" operator = "=">JohnDay</POR>
          <POR function = "or" operator = "=">BigEddy</POR>
     </PORList>
     <PODList function = "string">
          <POD function = "or" operator = "=">COB</POD>
          <POD function = "or" operator = "=">NOB</POD>
     </PODList>
     <ServiceList function = "string">
          <Service function = "or" operator = "=">
```

```
                <SERVICE_INCREMENT operator =
"=">hourly</SERVICE_INCREMENT>
                <TS_CLASS operator = "=">firm</TS_CLASS>
           </Service>
           <Service function = "or" operator = "=">
                <SERVICE_INCREMENT operator =
"=">hourly</SERVICE_INCREMENT>
                <TS_CLASS operator = "=">non-firm</TS_CLASS>
           </Service>
      </ServiceList>
</GetSchedule>
```

The method above would logically read:

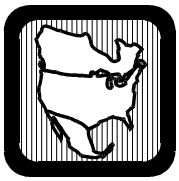
Give me all the schedules that have a flow between April 07, 2000 at 18:39:09 GMT and March 07, 2000, at 18:39:09 GMT
and a status of "Scheduled"
and a Upstream Control Area of AVA or BCHA or SCL
and a Downstream Control Area of CISO or LDWP
and a POR of JohnDay or BigEddy
and a POD of NOB or COB
and a Service of "Firm Hourly" or "Non-Firm hourly"

Of importance is that arrays of like elements are grouped together for purposes of evaluation in the query and that the function attribute on the array can affect on how the grouping is evaluated with respect to the previous accessor/parameter (be it an array, struct, or individual element). Within an array, the function and action attributes only effect the relationship among like elements within the array.

The response to the above GetSchedule method might look like:

```
<GetScheduleResponse xmlns="method-URI">
     <GetScheduleReturn>
          <SchedulesList>
               <Schedule>
                    <StartTime>####</StartTime>
                    <StopTime>####</StopTime>
                    <POR>#####</POR>
                    <POD>#####</POD>
                         *
                         *
                         *
                    <TCH>####</TCH>
                    <Capacity>
                         <Segment>
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                         <Segment>
```

```
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                         <Segment>
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                    </Capacity>
                    <Tag>
                         *
                         *
                         *
                    </Tag>
               </Schedule>
                    *
                    *
               <Schedule>
                    <StartTime>####</StartTime>
                    <StopTime>####</StopTime>
                    <POR>#####</POR>
                    <POD>#####</POD>
                         *
                         *
                         *
                    <TCH>####</TCH>
                    <Capacity>
                         <Segment>
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                         <Segment>
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                         <Segment>
                              <StartTime>####</StartTime>
                              <StopTime>####</StopTime>
                              <Level>####</Level>
                    </Capacity>
                    <Tag>
                         *
                         *
                         *
                    </Tag>
               </Schedule>
          </SchedulesList>
     </GetScheduleReturn>
</GetScheduleResponse>
```



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

OASIS Security Requirements

Developed by: OASIS Standards Collaborative (OSC)

DRAFT

January 6, 2001

INTENTIONALLY
BLANK

Table of Contents

1 INTRODUCTION 4

1.1 SCOPE 4
1.2 OVERVIEW 4
1.3 NOTATION CONVENTION 4

2 REQUIREMENTS 4

2.1 SSLV3.0 5
2.1.1 Encryption 5
2.1.2 Performance 5
2.1.3 Non-repudiation 5
2.2 CERTIFICATES 6
2.2.1 Server Certificates 6
2.2.2 Client Certificates 6
2.2.3 Certificate Authorities 6
2.3 CLIENT AUTHENTICATION 6
2.4 SERVER AUTHENTICATION 7
2.5 AUTHORIZATION 8
2.6 FIREWALLS, IP SECURITY, AND SERVER.HTM 8
2.7 LOGGING 8
2.8 NERC REGISTRY 9

3 APPENDIX A: RESOURCES 10

3.1 SPECIFICATIONS AND RFC 10
3.2 SSL/TLS TOOLKITS 10
3.3 HARDWARE AND INLINE ACCELERATORS 10
3.4 GENERAL LINKS AND BOOKS 11

4 APPENDIX B: CRYPTOGRAPHY AND SSLV3.0 OVERVIEW 12

4.1 CRYPTOGRAPHIC ALGORITHMS 12
4.1.1 Symetric Encryption 12
4.1.2 Asymetric Encryption 12
4.2 HASHING AND DIGESTING 13
4.3 DIGITAL SIGNATURES 14
4.4 KEY ESTABLISHMENT 15
4.5 DIGITAL CERTIFICATES 15
4.6 CERTIFICATE AUTHORITIES (CA) 16
4.7 SECURE SOCKETS LAYER (SSL/TLS) 17

1. Introduction

1.1 Scope

This document describes the security requirements for OASIS Phase 2, Electronic Tagging, and for any other industry systems that require strong security and authentication.

1.2 Overview

No formal method of securing communications among OASIS nodes, E-Tag nodes, or authenticating market participants has been available. The general consensus among OASIS administrators, market participants, and E-Tag participants is that if these systems were to be compromised, it would have a significant impact of system reliability and energy markets. The following security services were identified as the most critical:

1. Privacy: Messages are private among communicating parties.
2. Authentication: Determining whom you are communicating with.
3. Message Integrity: Ensuring that messages are not tampered with during transit.

Since both OASIS and E-Tag use HTTP 1.0/1.1, a technology capable of securing HTTP or the message content is necessary. Additionally, the technology chosen must be easily implemented and cost effective while still achieving the stated objectives (see section 2). The following security architecture is believed to meet these requirements and objectives:

1. Secure Sockets Layer, version 3.0.
2. Mutual Authentication (both Client and Server must have certificates and be authenticated)
3. 1024 bit X.509V3 certificates from approved commercial Certificate Authorities capable of supporting 128-bit SSLv3.0 encryption.

Additional details will be provided in the remainder of this document. **If unfamiliar with cryptographic concept or SSL, it is highly recommended that section 4 be reviewed first.**

1.3 Notation Convention

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.
A “CLIENT” shall be considered to be any system that initiates an SSL or HTTP connection/session. A “SERVER” shall be considered to be any system that accepts an SSL or HTTP connection/session and/or processes E-Tag methods.

2. Requirements

The requirements for OASIS security expand on the SSL/TLS security options provided under SMXP1.0, section 7.0. Review the SMXP1.0 specification for additional information regarding SSLv3.0 as it applies to the SMXP1.0.

2.1 SSLv3.0

ETag1.7 nodes (clients and servers) must use SSLv3.0 on IP port 443. Both client and server authentication (mutual) must be enabled. TLS1.0 may optionally be supported but must not be required by servers or clients.

2.1.1 Encryption

Secure Sockets Layer employs symmetric cryptography for the bulk encryption of session messages sent between the client and server. The session key for the bulk encryption of data shall be 128-bits long and the X.509v3 certificate used by a server must be capable of supporting a 128-bit key exchange. Conversely, the SSLv3.0 implementations (i.e., toolkits, operating system and libraries) utilized by both the client and server must be capable of supporting 128-bit encryption.

2.1.2 Performance

Depending on the cryptographic protocols being used and SSL parameters chosen, SSL connections can be anywhere between 2 and 100 times slower than ordinary TCP connections. To minimize the impact this may have on Electronic Tagging, there are several basic SSL performance rules that should be observed by clients and servers:

Asymetric Algorithm of choice: RSA

Symmetric Algorithm of choice: RC4 (128-bit). 3DES is more secure but has a significant performance penalty associated with it.

Digest Algorithm of choice: SHA-1. MD5 is slightly faster, but SHA-1 is more secure and MD5 is being phased out.

Session Resumption: Clients should always attempt to use session resumption[TWK3]. Servers should allow it if clients tend to reconnect within 5 to 10 minutes.

Record Size: Send data in the largest chunks possible.

Not all SSL/TLS toolkits and implementations may allow direct control over cryptographic settings and operating parameters. However, to the extent a client or server does have control over these operating parameters they should be set accordingly. The use of hardware or inline SSL accelerators may also be used to improve performance (see section 3.3). See section 4 for more information on cryptography and SSL.

2.1.3 Non-repudiation

SSL and TLS are not able to provide non-repudiation of data. While SSL/TLS ensures that communicating parties are certain of who they are talking to and provides for the highly secure and tamper proof transfer of data, the data itself is not signed with either of the communicating parties private keys. Consequently, outside of an SSL/TLS session, the data cannot stand-alone as non-repudiatable[TWK4]. Sufficient logging and vigilance on the part of both sender and receiver are necessary to adequately defend against possible claims repudiating data.

2.2 Certificates

Standard 1024-bit X.509v3 certificates (RFC 2459) shall be used by clients and servers.

2.2.1 Server Certificates

A server's certificate subject (i.e., distinguished name) shall have:

1. The "CN" field (Common Name) set to the fully qualified host name [TWK6]of the server.
2. The "OU" field (Organizational Unit) of the certificate's subject shall be set to the NERC registered code of the PSE/CA/TP associated with the server or that of a service provider acting on behalf of the PSE/CA/TP.
3. The "O" field (Organization) of the certificate's subject shall be the legal name of the entity represented by the NERC code located in the certificate's "OU" field.

The "CN", "OU" and "O" fields MUST be consistent with the NERC registry.

2.2.2 Client Certificates

A client certificate must be associated with a NERC registered PSE/CA/TP via the certificate's subject "OU" and "O" fields. The "CN" field of the certificate may either be the fully qualified host name [TWK7]of the client system communicating with the server or the name of an employee/individual authorized as a business representative by the NERC registered PSE/CA/TP.

2.2.3 Certificate Authorities

Client and server certificates may be acquired from any NERC approved Certificate Authority[TWK8] (see section 4.6 for description). The currently approved Certificate Authorities include[TWK9] [note: bogus list – need to evaluate several CA's yet]:

Certificate Authority	Product Name	Client	Server
ABC Certificates	ABC	Yes	No
Certificates "R" Us	DEF	Yes	No
Certificates "R" Us	GHI	No	Yes
Secure IT	JKL	No	Yes

2.3 Client Authentication

Servers must authenticate a client using the clients X.509v3 certificate. When establishing an SSLv3.0 session, the server shall request the clients certificate by issuing an SSLv3.0 CertificateRequest message to the client, per the SSLv3.0 specification (see Appendix B). In the event that a client attempts to establish a non-secure (i.e., port 80) HTTP session with the server (accept for "server.htm" file – section 2.6), the server must respond with an HTTP 403.4 error indicating that SSL is required.

The server must also perform the following certificate validation:

1. The certificate provided by the client must have had its subject and issuing Certificate Authority registered in the NERC Registry as detailed in section 2.8
2. In the event the client's certificate subject "CN" field is an IP address or host name, the server must verify that the client has initiated communications from the specified IP address or host.
3. The server must validate all certificates it receives by verifying the Certificate Authorities signature within them.
4. The server must check the validity period for all certificate, including the "not before" and "not after" times.

If any of these checks fail, the client shall not be permitted access and the server must return an HTTP 403 Forbidden.

The server shall also make a reasonable effort [TWK10]to check the current revocation status of any certificates before accepting them. This may be accomplished using a published Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP), provided by the Certificate Authority that signed the client certificate. If the certificate is determined to be revoked, suspended, or invalid, the server must cease communications with the client and return an HTTP 403 Forbidden. If a valid CRL cannot be obtained or an OCSP server contacted for more than 36 hours, the server must also cease communications with the client and return an HTTP 403 Forbidden.

Until the authentication failure is resolved, If the client attempts to continue to establish SSLv3.0 sessions, the server shall block the client from attempting further connections and notify the associated PSE/CA/TP and NERC.

2.4 Server Authentication

Clients shall only attempt to establish SSLv3.0 sessions and exchange production data with servers identified in the NERC Registry (see section 2.8). Clients may establish SSLv3.0 sessions for testing purposes with other servers provided that only non-sensitive data is exchanged and the intent is made clear.
The client must also perform the following certificate validation:

1. The host that communications has been established with must match the IP address or host name identified in the "CN" field of the certificate's subject.
2. The client must validate Certificate Authorities signature within the server's certificate.
3. The client must check the validity period of the server's certificate, including the "not before" and "not after" times.

Failing any of these checks, the client must cease communications and notify NERC.

The client shall also make a reasonable effort to check the current revocation status of the server's certificate. This may be accomplished using a published Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP), provided by the Certificate Authority that signed the client certificate. If the certificate is determined to be revoked, suspended or invalid, the client must cease communications. If a valid CRL for cannot be obtained or an OCSP server contacted for more than 36 hours, the client must also cease communications with the server.

2.5 Authorization

Assuming a client has been authenticated as described in section 2.3, the server shall authorize the client to perform only those operations allowed by the type of entity (PSE/CA/TP) they have been authenticated as and the security categories that the SO has authorized the certificate to perform (see section 2.8). The type of client shall be determined by cross-referencing the client's certificate subject with the NERC Registry. See the appropriate application specification (OASIS, E-Tag, etc.) for further information.

2.6 Firewalls, IP Security, and Server.htm

All Servers shall be placed behind a firewall. The firewall shall allow clients to access the server on port 443, the standard SSLv3.0 port. Client access to the server on IP ports other than 443 shall be restricted, except for a single HTML file on port 80. This HTML file shall be located at the root of the server and have a file name of "server.htm." This file shall allow anonymous access and contain the following information:

1. Server's host name
2. One or more administrative contacts including a 24 hour administrative contact (phone, fax, e-mail, pager)
3. Date/Time of the NERC Registry currently loaded.

Any unsecured links from "server.htm" shall only reference other sections of the file (server.htm) or files/resources on other servers. If images (gif and/or jpg) are included in this file, they should be served from a different server. Other html files and resources may be served from the server, and consequently reference in the "server.htm" file, as long as they are accessed via IP port 443 using SSLv3.0 and the client is authenticated using their certificate.

Since the firewall shall allow only IP ports 443 and 80, ICMP messages shall not be supported inbound, such as ping and trace-route. Outbound ICMP messages may still be performed. The html file located at "http://hostname:80/server.htm" , where "hostname" is the host name of the server in the NERC Registry, may be used to verify connectivity. As a substitute for ping, an HTTP TRACE on port 80 may also be performed to verify connectivity. Attempts to access the server on ports other than 443 and 80 shall be logged and include the date/time and IP address of the system attempting access. Firewall logs shall be kept for a minimum of 30 days after which they may be purged.

2.7 Logging

In addition to logs generated by the Firewall, the server shall log the following information for all messages/requests exchanged between the client and server (server may log additional information at its discretion):

1. Date and time to the millisecond that the server received the message/request.
2. Client's certificate full subject.
3. IP address of the client.
4. Success/Failure of the operation (http status codes)
5. Target URL of the client's message/request.
6. POST content of the client's message/request for any action that involves the creation of modification of data on the server. This is not necessary for query only operations.

This data must be maintained for a minimum of three (3) months and available upon request by NERC.

2.8 NERC Registry

Each market participant (PSE/CA/TP/Vendor) must establish a primary and backup Security Office (SO) with NERC. The SO shall be responsible for all modifications to data contained in the NERC registry for their company, including which certificates are authorized to perform specific market functions. This information shall ONLY be communicated to NERC by an authorized SO via out-of-band methods or by submittal of an authenticated message (secure e-mail or SSL). Acceptable out-of-band methods include:

1. Phone. NERC must call the SO back and challenge the SO with a previously established pass-phrase.
2. In person. SO must provide two authenticating credentials such as a valid drivers license and a company ID.

The registry shall contain the following security categories for each participant:

1. Tag: Produce, process, or approve tags.
2. Schedule: Schedule Energy or Transmission
3. Reserve: Reserve Transmission Capacity.
4. Market: Participation in other energy markets.
5. Other: As required or defined by NERC

In addition to other data currently required in the NERC Registry, all market participants and nodes must register with NERC the following information:

1. For each server function being performed, one or more fully qualified server host names. If a service provider is being used, it must be identified.
2. One or more client certificate subjects, [TWK12], their associated Certificate Authorities, and for which security categories they are authorized for (Tag, Schedule, Reserve, etc.). This is only appropriate or necessary when acting as a client.

In the case of a service provider, it is acceptable for the same server to provide services for more than one PSE/CA/TP or market participant. In this case, the same fully qualified host name will be provided by each PSE/CA/TP and the server may utilize the same server certificate.

NERC shall publish the full registry as a SHA-1/RSA digitally signed file [TWK13]using a client certificate obtained by NERC from one of the approved Certificate Authorities. Alternatively, the registry may be published in an SSL secured LDAP or HTTP server. Before relying on the registry obtained from NERC, both clients and servers (i.e., OASIS/E-Tag nodes) must verify the signature on the signed registry file (if used) and the validity of the certificate used to sign the registry. In the case of an SSL secured LDAP or HTTP server, the same checks as described in section 2.4 shall be used.

In the event the signature on the file or the certificate is found to be invalid or the authentication check of the LDAP or HTTP server fails, NERC shall be notified immediately and the last known valid registry shall continue to be used.

3. Appendix A: Resources

3.1 Specifications and RFC

Secure Sockets Layer (version 3.0)	http://www.netscape.com/eng/ssl3/
Transport Layer Security (RFC 2246)	http://www.ietf.org/rfc/rfc2246.txt
Key words use (RFC 2119)	http://www.ietf.org/rfc/rfc2119.txt
X.509v3 Certificate and CRL Profile (RFC 2459)	http://www.ietf.org/rfc/rfc2459.txt

3.2 SSL/TLS Toolkits

COMPANY	DESCRIPTION	URL
RSA Security	SSL/TLS/PKI toolkits - Java and C++	http://www.rsasecurity.com/products/bsafe/index.html
Baltimore	SSL/TLS/PKI toolkits - Java and C++	http://keytools.baltimore.com/ssl/index.html
DART	SSL/TLS toolkit – ActiveX/COM	http://www.dart.com/powertcp/
PHAOS Technology	SSL/TLS toolkit – Java	http://www.phaos.com/e_security/prod_ssl.html
Sun Microsystems	SSL/TLS toolkit – Java	http://java.sun.com/products/jsse/
OpenSSL	Open Source SSL/TLS toolkit – C++	http://www.openssl.org/
PureTLS	Open Source SSL/TLS toolkit – Java	http://www.rtfm.com/puretls/
Certicom	SSL/TLS tookit – Java and C	http://www.certicom.com/
IBM	PKIX Reference Implementation	http://www-3.ibm.com/security/library/wp_pkix.shtml
Mozilla.org	Cryptographic libraries	http://www.mozilla.org/projects/security/pki/psm/

3.3 Hardware and Inline Accelerators

COMPANY	DESCRIPTION	URL
Rainbow	CryptoSwift: PCI and Inline Accelerators	http://www.rainbow.com/

nCipher	nFast: PCI Accelerator	http://www.ncipher.com/
Intel	NetStructure: Inline Accelerator	http://www.intel.com/netstructure/ecommerce_equipment.htm
F5	E-Commerce Controller: Inline Accelerator	http://www.f5.com/

3.4 General Links and Books

LINKS	
PKI related links and resources	http://www.pki-page.org/
Encryption and Security-related Resources	http://www.cs.auckland.ac.nz/~pgut001/links.html
Introduction to SSL	http://developer.netscape.com/docs/manuals/security/sslin/contents.htm
PKI Forum	http://www.pkiforum.org/
PKI Guru	http://www.pkiguru.com/

BOOKS		
Title	**Author**	**ISBN**
SSL and TLS Essentials	Stephen Thomas	0-471-38354-6
SSL and TLS, Designing and Building Secure Systems	Eric Rescorla	0-201-61598-3
Internet Cryptography	Richard E. Smith	0-201-92480-3
Digital Certificates, Applied Internet Security	Jalal Feghhi, Jalil Feghhi, Peter Williams	0-201-30980-7

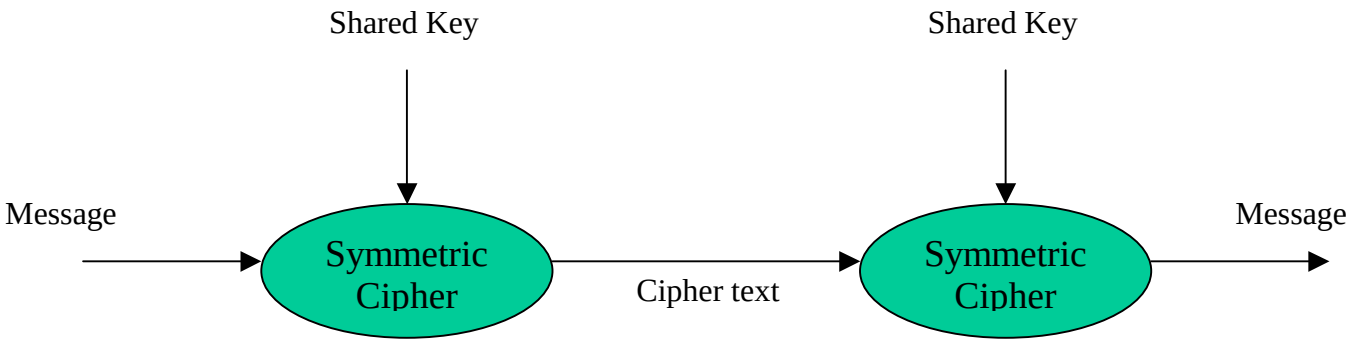
4. Appendix B: Cryptography and SSLv3.0 Overview

The books referenced in section 3 provide a complete description of public key infrastructures and the implementation of SSL and TLS. Below is a quick overview of how cryptographic algorithms, X.509v3 certificates and SSL/TLS work together.

4.1 Cryptographic Algorithms

4.1.1 Symetric Encryption

Secret Key Cryptography is commonly referred to as "symmetric encryption."
When utilizing symmetric cipher, both sender and receiver have the "shared key" and it is used for both encryption and decryption.



Common symmetric key ciphers:

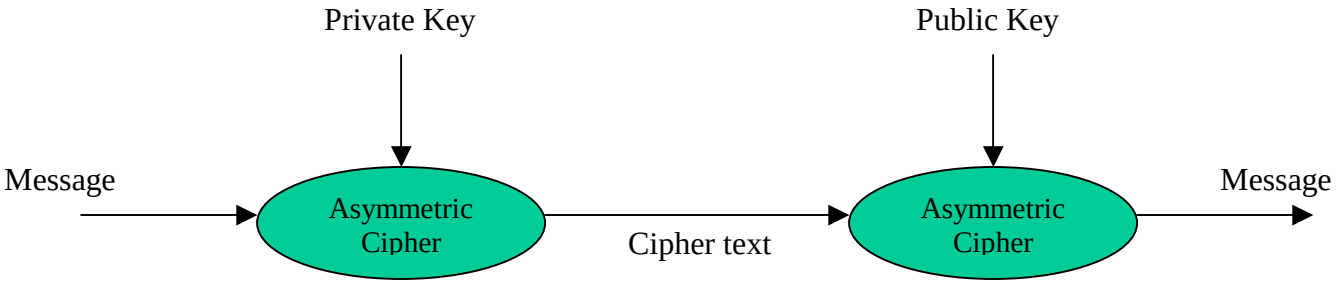
•DES: Data Encryption Standard (56 bit block cipher)
•3DES: Triple-Strengths Data Encryption Standard (112 bit block cipher)
•RC2: Rivest Cipher 2 (variable key length block cipher)
•RC4: Rivest Cipher 4 (variable key length stream cipher)

Note1: RC4 is extremely fast; a Pentium II/400 can achieve speeds on the order of 45 MB/s. RC2 and 3DES, however, are many times slower.

Note2: The US National Institute of Standards and Technology (NIST) has selected the Advanced Encryption Standard [TWK14](AES) to replace DES as the US government's standard encryption algorithm.

4.1.2 Asymetric Encryption

Public Key Cryptography is commonly referred to as "asymmetric cryptography." The two primary uses of public key cryptography are key establishment (section 4.4) and digital signatures (section 4.3). When utilizing an asymmetric cipher, messages are encrypted by one of the key pairs and decrypted with the other.



In the example above, the private key is closely guarded by the sender and never shared. The receiver only knows the public key that corresponds to the private key used to encrypt the message. Alternatively, a message may be encrypted using a public key and may then only be decrypted by the private key.

Common Asymmetric key ciphers/algorithms:

•DSA/DSS: Digital Signature Algorithm (type: Digital Signature)
•El Gamal: (type: Digital Signature)
•RSA: Rivest, Shamir, Adleman (type: Signature, encryptions, key exchange)
•Diffie-Hellman: (type: Key exchange)

4.2 Hashing and Digesting

A **Message-digest algorithm** take a variable-length message as input and produces a fixed-length digest as output. The fixed length output is called the "**message-digest**", "the **digest**" or a "**hash**." The algorithms are also referred to as a "**one-way hash algorithm**" or simply a "**hash algorithm**." A message digest algorithm must satisfy four properties:

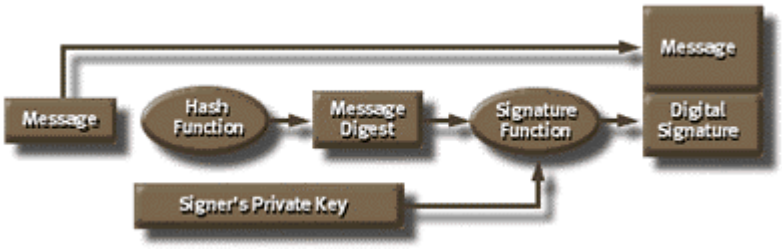
1. In must not be feasible to determine the input message based on its digest.
2. In must not be possible to find an arbitrary message that has a particular, desired digest.
3. Should be computationally infeasible to find two messages that have the same digest.
4. Mappings from a message to a digest should appear random and flipping even one bit of the message results in an entirely new and uncorrelated digest.

Message-Digest Algorithm	Digest Length (bits)
MD2	128
MD4	128
MD5	128
SHA	160
SHA-1	160

Note: MD5 and SHA-1 are newer algorithms and generally used by SSL and TLS. MD5 has an approximate 2 to 1 speed advantage over SHA-1, but MD5 is slowly being phased out.

4.3 Digital Signatures

In order to sign a message, the message originator creates a message digest and signs (encrypts) the digest with their private key. The original message and the signed hash are then sent to the recipient(s).



Recipient(s) uses the same hash function on the message as the signer. Recipient(s) then uses the signer's public key to decrypt the message digest the originator signed. If the message digests are identical, the signature will verify and one can safely assume the message came from the signer and has not been altered or counterfeited.

Note: Currently **RSA** and **DSS** are commonly used to create digital signatures. DSS was invented by the NSA (FIPS-186) and uses the SHA-1 digest algorithm. RSA, however, may use any digest, such as MD5.

4.4 Key Establishment

Two types of key establishment exist, *key exchange (*also known as a *key transport)* and *key agreement*. In the case of key exchange, one side generates a symmetric key, encrypts it using a public key of the other side, and then sends it to the other side. In *key agreement*, both sides cooperate to generate a shared key.

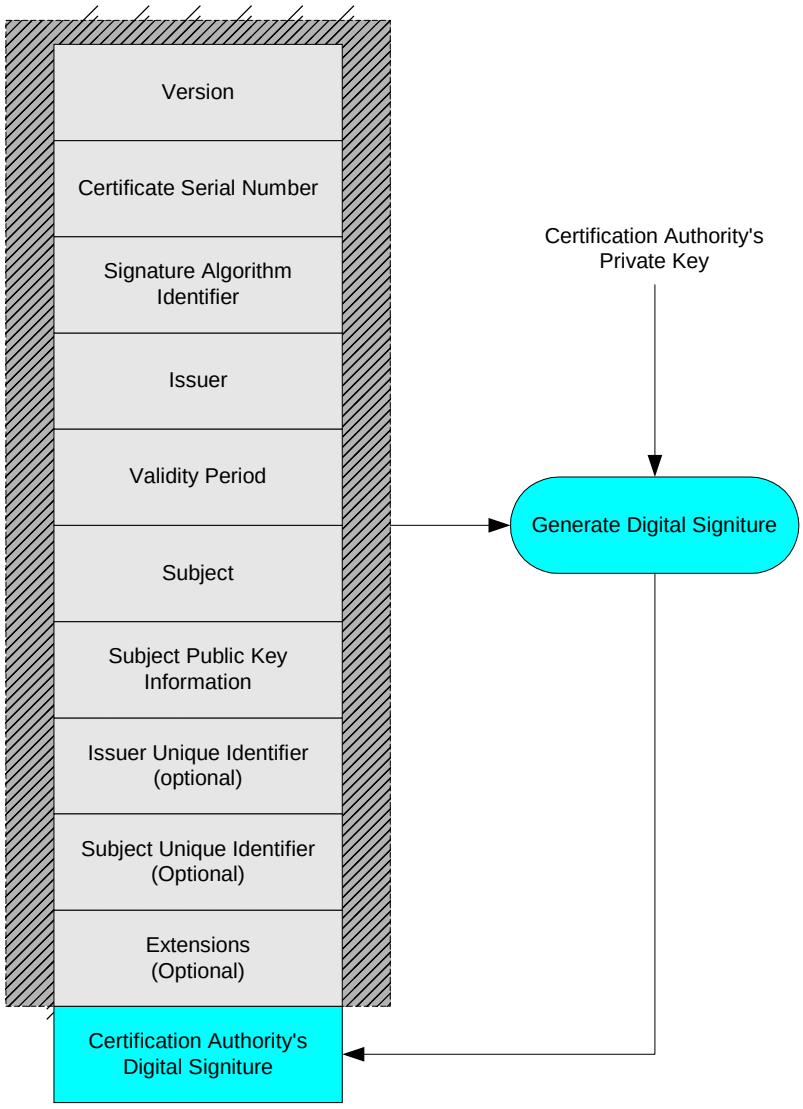
Cryptographic Algorithms supporting Key Establishment:

- **RSA**: (Rivest, Shamir, Adelman) Supports *key exchange*.
- **DH**: (Diffie-Hellman) Supports *key agreement*.

4.5 Digital Certificates

Certificates are electronic documents that correlate (called binding) a public key with a specific entity. Commonly this entity is a person but may be a computer, software, document, etc. Certificates may be used to authenticate persons in a SSL session, to encrypt messages or digitally sign messages. Digital Certificates contain, among other things, the following information:

- **Version:** Contains the version number of the encoded certificate (currently 1, 2, or 3).
- **Serial Number:** A unique number assigned by the CA
- **Signature Algorithm:** Algorithm used by the CA to digitally sign the certificate (RSA or DSA)
- **Issuer Name:** The CA who has signed the certificate
- **Validity Period:** Time interval during which the certificate is valid.
- **Subject Name:** This is the identity of the entity whose public key is certified in the public key. Sometime called a Distinguished Name (DN).
- **Subject Public Key Information:** Contains public key and parameters.
- **Issuer unique identifier:** Optional field to allow the reuse of issuer names over time.
- **Subject unique identifier:** Optional field to allow the reuse of the subject name over time.
- **Extensions:** Way to associate additional information for subjects, public keys, etc.



X.509 v3 Certificate Format

By signing a certificate, a Certificate Authority if acting as a trusted third-party and certifying that the contents of the certificate are verifiably correct.

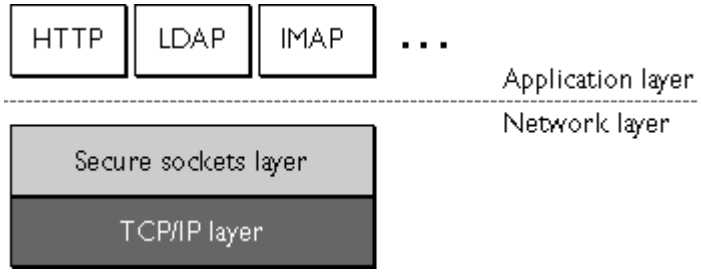
4.6 Certificate Authorities (CA)

Typically a CA verifies the credentials of entities seeking certificates, issue them, and then make these certificates available in some common database (usually a directory.) CAs must be trusted in order for their certificates to be meaningful. A very large PKI may also include an RA, or Registration Authority, or even a LRA or Local Registration Authority that does actual physical verification.

A CRL is a Certificate Revocation List. CRLs are regularly created, signed, and published by CAs in order to list certificates that have been compromised or revoked prior to the certificates expiration date. A CA may also provide a server or system that may be queried using the Online Certificate Status Protocol (OCSP). This type of service provides for real-time certificate status checking. Most CRLs are published only once or twice a day.

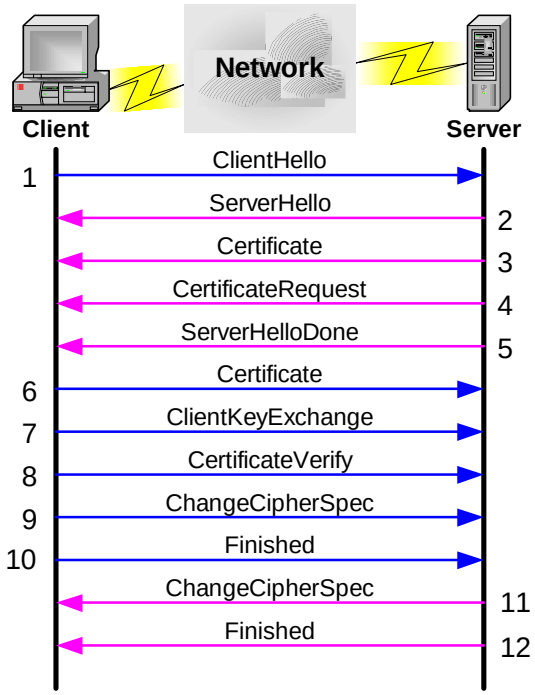
4.7 Secure Sockets Layer (SSL/TLS)

SSLv3 (version 3) is functionally a security protocol that fits between the application layer and TCP. As such, it can secure many different application layer protocols such as HTTP, FTP, Telnet, etc.



Originally developed by Netscape, the protocol was eventually turned over to the Internet Engineering Task Force (IETF). In January 1999, the Transport Layer Security (TLS) protocol was published by the IETF (RFC 2246). The Transport Layer Security protocol (TLS) is the successor to SSLv3. It should be considered the next version of SSL and is currently at version 1.0. Inside the TLS/SSL hello message, an SSLv3 session is identified as version 3.0 and a TLS session is identified as version 3.1.

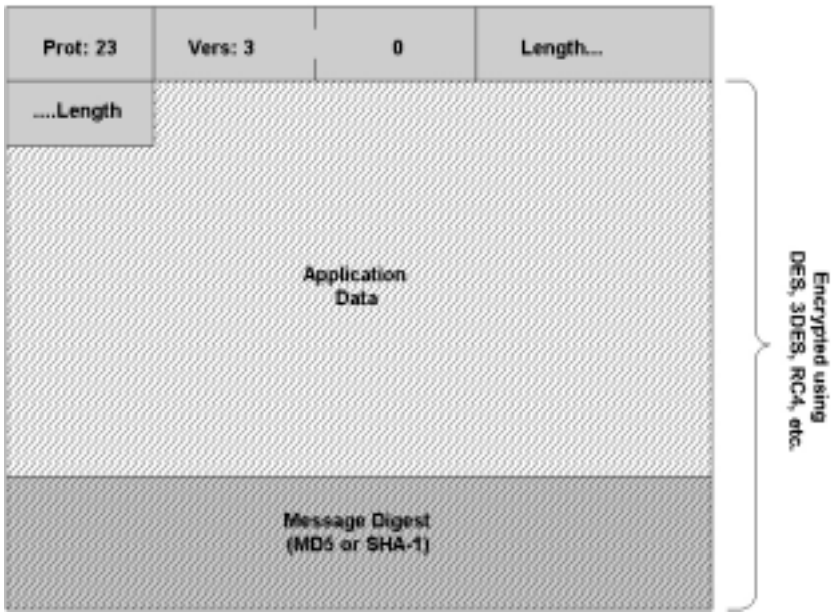
In SSL and TLS, there is always a "client" role and a "server" role. The message protocol when both client and server authentication are enforced is as follows:



Step 1: Client sends ClientHello message proposing SSL options such as version and cipher algorithms supported.
Step 2: Server responds with a ServerHello message selecting the SSL options to use.
Step 3: Server sends its public key certificate in the Certificate Message

Step 4: Server sends a CertificateRequest message to indicate that it wants to authenticate the client.
Step 5: Server concludes its part of the negotiation with a ServerHelloDone message.
Step 6: Client sends its public key certificate in a Certificate message.
Step 7: Client sends session key information (encrypted with the servers public key) in a ClientKeyExchange message.
Step 8: Client sends CertificateVerify message, which signs important information about the session using the client's private key; the server uses the public key from the client's certificate to verify the client's identity.
Step 9: Client sends a ChangeCipherSpec message to activate the negotiated options for all future message it (the client) will send.
Step 10: Client sends a Finished message to let the server check the newly activated options.
Step 11: Server sends a ChangeCipherSpec message to activate the negotiated options for all future messages it (the server) will send.
Step 12: Server sends a Finished message to let the client check the newly activated options.
SSL is now ready for the application to use as an authenticated, high integrity, secure and private communications channel.

An SSL message:



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Certificate Policy
for
Energy **M**arket **A**ccess
and
Reliability **C**ertificates
(**e-MARC**)

DRAFT
Version 0.3

North American Electric Reliability Council
February 7, 2001

Table Of Contents

Section **Page**

SECTION 1 INTRODUCTION 1

1.1 OVERVIEW 1
1.2 POLICY IDENTIFICATION 1
1.3 COMMUNITY AND APPLICABILITY 2
1.3.1 Certification Authorities (CAs) 2
1.3.2 Registration Authorities (RAs) 2
1.3.3 Certificate Manufacturing Authorities (CMAs) 3
1.3.4 Repositories 3
1.3.5 End Entities 3
1.3.6 Policy Authority 4
1.3.7 Applicability and Applications 4
1.4 CONTACT DETAILS 5
1.4.1 Policy Administration Organization 5
1.4.2 Contact Person 5
1.4.3 Person Determining e-MARC CPS Suitability for the Policy 5

SECTION 2 GENERAL PROVISIONS 6

2.1 OBLIGATIONS 6
2.1.1 Authorized CA Obligations 6
2.1.2 RA Obligations 7
2.1.3 CMA Obligations 7
2.1.4 Repository Obligations 7
2.1.5 Subscriber Obligations 7
2.1.6 Qualified Relying Party Obligations 8
2.1.7 Policy Authority Obligations 8
2.2 LIABILITIES 8
2.2.1 Authorized CA Liability 9
2.2.2 RA, CMA, and Repository Liability 9
2.3 FINANCIAL RESPONSIBILITY 9
2.3.1 Indemnification by Relying Parties 9
2.3.2 Fiduciary Relationships 9
2.3.3 Administrative Processes 9
2.4 INTERPRETATION AND ENFORCEMENT 9
2.4.1 Governing Law 9
2.4.2 Severability, Survival, Merger, Notice 9
2.4.3 Dispute Resolution Procedures 9
2.5 FEES 10
2.5.1 Certificate Issuance, Renewal, Suspension, and Revocation Fees 10
2.5.2 Certificate Access Fees 10
2.5.3 Revocation Status Information Access Fees (Certificate Validation Services) 10
2.5.4 Fees for Other Services such as Policy Information 10
2.5.5 Refund Policy 10
2.6 PUBLICATION AND REPOSITORY 11
2.6.1 Publication of Information 11
2.6.2 Frequency of Publication 11

2.6.3 Access Controls 11
2.6.4 Repositories 11
2.7 QUALITY ASSURANCE INSPECTION AND REVIEW 11
2.7.1 Frequency of Certification Authority Compliance Review 11
2.7.2 Identity/Qualifications of Reviewer 11
2.7.3 Auditor's Relationship to Audited Party 12
2.7.4 Topics Covered by Quality Assurance Inspection and Review 12
2.7.5 Actions Taken as a Result of Deficiency 12
2.7.6 Communication of Results 12
2.8 CONFIDENTIALITY 13
2.8.1 Types of Information to Be Kept Confidential 13
2.8.2 Types of Information Not Considered Confidential 13
2.8.3 Disclosure of Certificate Revocation/Suspension Information 13
2.8.4 Release to Law Enforcement Officials 13
2.8.5 Release as Part of Civil Discover 14
2.8.6 Disclosure upon Owner's Request 14
2.8.7 Other Information Release Circumstances 14
2.9 INTELLECTUAL PROPERTY RIGHTS 14

SECTION 3 IDENTIFICATION AND AUTHENTICATION 15

3.1 INITIAL REGISTRATION 15
3.1.1 Types of Names 15
3.1.2 Name Meanings 15
3.1.3 Rules for Interpreting Various Name Forms 16
3.1.4 Name Uniqueness 16
3.1.5 Name Claim Dispute Resolution Procedures 16
3.1.6 Recognition, Authentication, and Role of Trademarks 16
3.1.7 Verification of Possession of Key Pair 16
3.1.8 Authentication of Sponsoring Organization Identity 16
3.1.9 Authentication of Individual Identity 17
3.2 ROUTINE REKEY (RENEWAL) 18
3.3 REKEY AFTER REVOCATION 18
3.4 REVOCATION REQUEST 18

SECTION 4 OPERATIONAL REQUIREMENTS 19

4.1 CERTIFICATE APPLICATION 19
4.2 CERTIFICATE ISSUANCE 19
4.3 CERTIFICATE ACCEPTANCE 19
4.4 CERTIFICATE SUSPENSION AND REVOCATION 20
4.4.1 Who Can Request Revocation 20
4.4.2 Circumstances for Revocation 20
4.4.3 Procedure for Revocation Request 21
4.4.4 Revocation Request Grace Period 21
4.4.5 Circumstances for Suspension 21
4.4.6 Who Can Request Suspension 21
4.4.7 Procedure for Suspension Request 21
4.4.8 Limits on Suspension Period 21
4.4.9 CRL Issuance Frequency 21
4.4.10 CRL Checking Requirements 21
4.4.11 Online Revocation/Status Checking Availability 22

4.4.12 Online Revocation Checking Requirements 22
4.4.13 Other Forms of Revocation Advertisements Available 22
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements 22
4.4.15 Special Requirements re Key Compromise 22
4.5 COMPUTER SECURITY AUDIT PROCEDURES 22
4.6 RECORDS ARCHIVAL 22
4.6.1 Types of Events Recorded 22
4.6.2 Retention Period for Archive 23
4.6.3 Protection of Archive 23
4.7 KEY CHANGEOVER 23
4.8 COMPROMISE AND DISASTER RECOVERY 24
4.8.1 Computing Resources, Software, and/or Data are Corrupted 24
4.8.2 Authorized CA Public Key Is Revoked 24
4.8.3 Authorized CA Private Key Is Compromised (*Key Compromise Plan*) 24
4.8.4 Secure Facility after a Natural or Other Disaster (*Disaster Recovery Plan*) 24
4.9 AUTHORIZED CA CESSATION OF SERVICES 25
4.10 CUSTOMER SERVICE CENTER 25

SECTION 5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS .. 26

5.1 PHYSICAL SECURITY CONTROLS 26
5.2 PROCEDURAL CONTROLS 26
5.2.1 Trusted Roles 26
5.2.2 Number of Persons Required Per Task 26
5.2.3 Identification and Authentication for Each Role 26
5.3 PERSONNEL SECURITY CONTROLS 27

SECTION 6 TECHNICAL SECURITY CONTROLS 28

6.1 KEY PAIR GENERATION AND INSTALLATION 28
6.1.1 Key Pair Generation 28
6.1.2 Private Key Delivery to Entity 28
6.1.3 Subscriber Public Key Delivery to Authorized CA 28
6.1.4 Authorized CA Public Key Delivery to Users 28
6.1.5 Key Sizes 28
6.2 AUTHORIZED CA PRIVATE KEY PROTECTION 28
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 29
6.3.1 Public Key Archival 29
6.3.2 Usage Periods for the Public and Private Keys (*Key Replacement*) 29
6.4 ACTIVATION DATA 29
6.5 COMPUTER SECURITY CONTROLS 29
6.7 NETWORK SECURITY CONTROLS 29
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 29

SECTION 7 CERTIFICATE AND CRL PROFILES 30

7.1 CERTIFICATE PROFILE 30
7.2 CRL PROFILE 30

SECTION 8 POLICY ADMINISTRATION 31

8.1 POLICY CHANGE PROCEDURES 31

8.1.1 List of Items 31
8.1.2 Comment Period 31
8.2 PUBLICATION AND NOTIFICATION PROCEDURES 31
8.3 CPS APPROVAL PROCEDURES 31

GLOSSARY 32

Section 1

Introduction

1.1 OVERVIEW

In support of deregulated energy markets and system reliability function, many computer-based systems, applications, and market participants have a significant requirement for the secure operations of these networked computer-based systems, electronic messages, and transactions. Fulfilling that requirement requires the use of digital signatures to ensure:

- **P**rivacy: No one other than the parties or systems involved will know the details of the of electronic messages;
- **A**uthentication: All parties to a transaction or electronic message exchange will know at the outset who they are dealing with;
- **I**ntegrity: Messages cannot be changed while in transit between parties or systems; and
- **N**on-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

This requires the use of public key cryptography and public key certificates to bind a person's or computer system's public key to his/her/its identity and to support symmetric encryption key exchange. In support of this goal, the North America Electric Reliability Counsel (NERC) will provide for commercial public key certificate services to the deregulated energy markets and system reliability function (referred to as "Energy Market Access and Reliability Certificates " or "e-MARC"). NERC will do this by certifying Registry Domains, Registry Administrations, and service provider(s) to provide the services presented in this policy.

This Certificate Policy ("Policy" or CP) describes (1) roles, responsibilities, and relationships among the Registry Domains, Registry Administrators, Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified Relying Parties, and Policy Authority (referred to collectively as "Program Participants") authorized to participate in the public key infrastructure described by this Policy, (2) the primary obligations and operational responsibilities of the Program Participants, and (3) the rules and requirements for the issuance, acquisition, management, and use of an e-MARC to verify digital signatures.

This Certificate Policy (CP) provides a high level description of the policies and operation of the e-MARC Program and follows the X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as detailed in RFC 2527 of the IETF. Specific detailed implementations of this policy will be found in the Certificate Practice Statement (CPS) of any Certificate Authority certified to issue certificates bound by this policy.

1.2 POLICY IDENTIFICATION

This Policy is registered with the _____ and has been assigned the following object identifiers (OIDs) for the e-MARC Certificates defined in this Policy.

Identity e-MARC Certificates: { _____ }
Business Representative e-MARC Certificates: { _____ }

Server e-MARC Certificates: { _____ }
Qualified Relying Party Application e-MARC Certificates: { _____ }

All e-MARC Certificates issued under this Policy shall reference this Policy by including the appropriate OID for this Policy in the *Certificate Policies* field of the e-MARC Certificate. The foregoing OIDs may not be used except as specifically authorized by this Policy.

1.3 COMMUNITY AND APPLICABILITY

This Policy describes a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under this Policy to fulfill any of the following roles: Registry Service Provider roles, Certificate Service Provider roles, End Entity roles, and Policy Authority role. Registry Service Provider role are Registry Administrators. Certificate Service Provider roles are Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository. End Entity roles are Subscriber and Relying Party. Requirements for persons and entities authorized to fulfill any of these roles are in this Section. A general description of each of these roles and their responsibilities is set forth in Section 2 of this Policy.

1.3.1 Registry Domains

A Registry Domain may participate in this Policy only if qualified and authorized to do so by the Policy Authority. In order to qualify as an authorized Registry Domain, the Registry must:

(a) be a registry of organizations participating in an energy market;
(b) include an organizations DUNS number as one of their attributes; and
(c) assign a unique alphanumeric code (Entity Code) to all registered organizations.

1.3.2 Registry Administrators

A Registry Administrator may participate in this Policy and administer a qualified and authorized Registry Domain only if such Registry Administrator first qualified as an authorized Registry Administrator by:

(a) entering into an appropriate e-MARC Contract;
(b) documenting the specific practices and procedures that it will implement to satisfy the requirements of this Policy and of the Registry Domain they wish to administer.

1.3.3 Certification Authorities (CAs)

A CA may issue certificates that identify this Policy ("e-MARC Certificates") only if such CA first qualifies as an "Authorized CA" by:

(a) entering into an appropriate e-MARC Contract;
(b) documenting the specific practices and procedures it will implement to satisfy the requirements of this Policy in a certificate practice statement ("e-MARC CPS"); and
(c) successfully completing e-MARC Security Certification and Accreditation.

1.3.4 Registration Authorities (RAs)

Each Authorized CA shall perform the role and functions of the Registration Authority (RA). An

Authorized CA may subcontract Registration Authority functions to third party RAs who agree to be bound by this Policy, provided that each such subcontractor is approved in advance by the NERC, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its NERC e-MARC Contract. The only exception is when the NERC, pursuant to agreement between NERC, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

1.3.5 Certificate Manufacturing Authorities (CMAs)

Each Authorized CA shall perform the role and functions of the Certificate Manufacturing Authority (CMA). An Authorized CA may subcontract CMA functions to third party CMAs who agree to be bound by this Policy, provided that each such subcontractor is approved in advance by NERC, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its NERC e-MARC Contract.

1.3.6 Repositories

Each Authorized CA shall perform the role and functions of the Repository. An Authorized CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by NERC, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its NERC e-MARC Contract.

1.3.7 End Entities

An Individual or organization and their agents may be Subscribers or Qualified Relying Parties. As described in sections 1.3.7.1 Subscribers and 1.3.7.2 Qualified Relying Parties, Subscribers may be issued e-MARC Certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability is attributable to an individual or an organization.

e-MARC Certificates will only be issued after requests or authorization for issuance from one or more Sponsors. They may be issued to employees, citizens, organizations and others with whom the Sponsor has a relationship.

Eligibility for a certificate is at the sole discretion of the CA and a CA may administer any number of Subscribers.

1.3.7.1 Subscribers

An Authorized CA may issue e-MARC Certificates to the following classes of Subscribers:

(a) Members of the general public ("Unaffiliated Individuals");
(b) Individuals authorized to act on behalf of business entities (i.e., Sponsoring Organizations registered in an authorized Registry) recognized by the Authorized CA, such as employees, officers, and agents of a Sponsoring Organization ("Business Representatives");
(c) Servers, devices, and/or computer applications that may take action on behalf of a business entity (i.e., Sponsoring Organizations registered in an authorized Registry) recognized by the Authorized CA, such as, but not limited to, web servers, application servers, and custom client applications.
(d) Qualified Relying Parties that choose to use e-MARC.

1.3.7.2 Qualified Relying Parties

Persons and entities authorized to accept and rely upon e-MARC Certificates for purposes of privacy, authentication, integrity, and non-repudiation of electronic records and messages are those eligible entities that enter into an e-MARC Agreement (i.e., Memorandum of Understanding) to accept e-MARC Certificates and agree to be bound by the terms of this Policy ("Qualified Relying Parties"). Eligible entities include all recognized energy market participant registered in an authorized Registry, Federal agencies, State and local agencies, authorized contractors and sponsored universities and laboratories of the Policy Authority, and other organizations as deemed appropriate under this policy and by the Policy Authority. The Policy Authority has the right to add authorized users in these categories at any time during the term of this Policy.

1.3.8 Policy Authority

The NERC serves as the Policy Authority and is responsible for organizing and administering the e-MARC Policy and e-MARC Contract (s).

1.3.9 Applicability and Applications

1.3.9.1 Purpose

Subscribers and Authorized CAs may use e-MARC Certificates to authenticate Subscribers to Qualified Relying Party applications for individual and/or business purposes, and for authentication of Qualified Relying Party applications. The following table summarizes the functional uses of e-MARC Certificates:

e-MARC Certificate Type	Subscriber	Use of Certificate
Unaffiliated Individual	Unaffiliated Individual	To enable an Unaffiliated Individual to authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Business Representative	Business Representative authorized to act on behalf of a Sponsoring Organization	to authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Device (SSL)	Servers, devices, and/or computer applications authorized to act on behalf of a Sponsoring Organization	to authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Qualified Relying Party Application (OCSP/CRL)	Qualified Relying Party	To enable a Qualified Relying Party to authenticate itself to Unaffiliated Individuals, Business Representatives, and Authorized CAs and to verify digitally signed documents/transactions

1.3.9.2 Suitable Applications

e-MARC Certificates may be, but are not limited to, use in the following suitable applications:

(a) Energy Market transactions;
(b) Energy or Transmission Scheduling;
(c) Filings with government agencies;
(d) Filings with law enforcement agencies;
(e) Application processes, such as applying for or requesting access to physical facilities;
(f) Financial transactions within the energy markets community;
(g) Billing, Metering, and Invoicing;
(h) Conveyance and transfer or operational data; and
(i) Conveyance and transfer or system reliability data.

1.3.9.3 Restricted and Prohibited Applications

e-MARC Certificates shall NEVER be used for:

(a) Any transaction or data transfer that if compromised or falsified may cause physical injury or loss of life.
(b) Any transaction or data transfer that if compromised or falsified may result in imprisonment.
(c) Any transaction or data transfer deemed illegal under federal law.
(d) The bulk encryption of data or documents using the certificates public or private key. (Bulk encryption may be accomplished using symmetric key cipher algorithms with the e-MARC certificate used for secure key exchange use only)

1.4 CONTACT DETAILS

1.4.1 Policy Administration Organization

NERC, as the Policy Authority and Contract Authority, administers this Policy:

North American Electric Reliability Counsel
116-390 Village Boulevard
Princeton, New Jersey 08540-5731

1.4.2 Contact Person

Attn.: e-MARC Administrator
Phone: (XXX) XXX-XXXX
e-mail address: emarc.policy@nerc.com

1.4.3 Person Determining e-MARC CPS Suitability for the Policy

Attn.: e-MARC Administrator
Phone: (XXX) XXX-XXXX
e-mail address: emarc.policy@nerc.com

Section 2

General Provisions

2.1 OBLIGATIONS

This Section provides a general description of the roles and responsibilities of the e-MARC Program Participants operating under this Policy: Authorized Registration Domains, Registry Administrators, Authorized CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Qualified Relying Parties, and the Policy Authority. Additional obligations are set forth in other provisions of this Policy, the NERC e-MARC Contracts, the e-MARC Agreements with Qualified Relying Parties, and the Subscriber Agreements.

2.1.1 Registry Domains Obligations

A Registry Domain is responsible for containing a list of organizations that are authorized to participate in a particular energy market or reliability function and recognized by other participants in that market. It is the obligations of a Registry Domain to:

(a) Have documented and enforceable requirements for market participants;
(b) obtain and maintain a registered Internet domain name to uniquely identify the registry;
(c) include an organizations DUNS number in the registration;
(d) assign an unique alphanumeric "Entity Code" to each registered organization; and
(e) make all entries electronically and reliably available to all e-MARC Program Participants.

2.1.2 Registry Administrator Obligations

It is the responsibility and obligation of a Registry Administrator to ensure that the Registry Domain for which they have been authorized to administer and maintain by the Policy Authority meets its obligations under this policy and:

(a) registering market participant in the registry and managing the application/enrollment process;

(b) the identification and verification process to ensure they are an eligible market participant in accordance with the Registry Domain's policies;

(c) In accordance with the Certificate Revocation requirements of this Policy, promptly notifying all authorized Certification Authorities (CA) of registration changes or modifications that affect the status of e-MARC certificates issued to registered organization.

2.1.3 Authorized CA Obligations

This Policy describes the responsibilities on each Authorized CA that issue e-MARC Certificates (and all of its subcontractor RAs, CMAs, and Repositories) by virtue of its NERC e-MARC Contract, and governs its performance with respect to all e-MARC Certificates it issues.

Each Authorized CA/RA is responsible for all aspects of the issuance and management of e-MARC Certificates, including the application/enrollment process; the identification verification and authentication process; the certificate manufacturing process; dissemination and activation of the certificate; publication of the certificate (if required); renewal, suspension, revocation, and replacement of the certificate; verification of certificate status upon request; and ensuring that all aspects of the Authorized CA Services and Authorized CA operations and infrastructure related to e-MARC Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. The only exception is when the Policy Authority, pursuant to agreement between the Policy Authority, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

2.1.4 RA Obligations

A Registration Authority (RA) is responsible for the applicant registration, certificate application, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, and Qualified Relying Parties. An RA may also be responsible for handling suspension and revocation requests, and for aspects of Subscriber education.

2.1.5 CMA Obligations

A Certificate Manufacturing Authority (CMA) is responsible for the functions of manufacturing, issuance, suspension, and revocation of e-MARC Certificates.

2.1.6 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving e-MARC Certificates, a current copy of this Policy, and other information relevant to e-MARC Certificates, and for providing information regarding the status of e-MARC Certificates as valid or invalid that can be determined by a Qualified Relying Party.

2.1.7 Subscriber Obligations

The responsibilities of each applicant for an e-MARC Certificate are to:

- provide complete and accurate responses to all requests for information made by the Authorized CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes;
- generate a key pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key;
- upon issuance of an e-MARC Certificate naming the applicant as the Subscriber, review the e-MARC Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the e-MARC Certificate;
  use the e-MARC Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy;
- instruct the issuing Authorized CA (or an authorized RA) to revoke the e-MARC Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of a Device or Business Representative e-MARC Certificate, whenever the Subscriber or Device is no longer affiliated with the Sponsoring Organization or the Device is no longer active; and
- Instruct the issuing Authorized CA (or an authorized RA) to revoke the e-MARC Certificate promptly upon a change of an Individual or Sponsoring Organization's registration in the

Registry Domain (where applicable). Changes in registration include DUNS number or Entity Code, or any other attribute that the appropriate Registry Administrators deems to warrant revocation and is in accordance with the policy.

2.1.8 Qualified Relying Party Obligations

This Policy is binding on each Qualified Relying Party by virtue of its e-MARC Agreement, and governs its performance with respect to its application for, use of, and reliance on e-MARC Certificates.

(a) Acceptance of Certificates. Each Qualified Relying Party will validate e-MARC Certificates issued by all Authorized CAs;

(b) Certificate Validation. Each Qualified Relying Party will validate every e-MARC Certificate it requests and receives with the Authorized CA that issued the certificate; and

(c) Reliance. A Qualified Relying Party may rely on a valid e-MARC Certificate for purposes of verifying the digital signature and symmetric key exchange only if:

- The e-MARC Certificate was used and relied upon to authenticate a Subscriber's digital signature for an application bound by this Policy;
- Prior to reliance, the Qualified Relying Party (1) verified the digital signature by reference to the public key in the e-MARC Certificate, and (2) checked the status of the e-MARC Certificate by checking a current CRL or by generating an online status request, through OCSP, to the issuing Authorized CA, and a check of the certificate's status indicated that the certificate was valid; and
- The reliance was reasonable and in good faith in light of all the circumstances known to the Qualified Relying Party at the time of reliance.

2.1.9 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy, contract administration, and the authorization and approval of Registry Domains, Registry Administrators, Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, and Repositories to participate in this Policy.

2.2 LIABILITIES

Nothing in this Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on any Program Participant by virtue of any contract or obligation that is otherwise determined by applicable law.

2.2.1 Authorized CA Liability

Except as otherwise provided in this CP, an Authorized CA may limit its maximum potential liability through contractual agreement with the Policy Authority, Subscribers and/or Qualified Relying Parties, in its CPS, or in Certificates by stating a reliance limit, and may further limit direct losses or damages to exclude those occasioned by circumstances outside or beyond its direct control, including any direct, indirect, consequential, incidental, special, exemplary or punitive damages.

2.2.2 RA, CMA, and Repository Liability

See 2.2.1.

2.3 FINANCIAL RESPONSIBILITY

Not yet defined

2.3.1 Indemnification by Relying Parties

Not yet defined.

2.3.2 Fiduciary Relationships

Not yet defined.

2.3.3 Administrative Processes

Not yet defined.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The laws of the United States shall govern the enforceability, construction, interpretation, and validity of this Policy.

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

In the event of any dispute or disagreement between two or more of the Program Participants ("Disputing Parties") arising out of or relating to this Policy or e-MARC Contracts, CPS, or Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s). If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties may present the dispute to the e-MARC Contract Officer for resolution.

Any contract dispute between Authorized CAs and e-MARC Contract Officer shall be handled under the terms and conditions of the e-MARC contract.

2.5 FEES

2.5.1 Certificate Issuance, Renewal, Suspension, and Revocation Fees

The Authorized CA may impose a fee to issue or renew e-MARC certificates. The Authorized CA shall not impose a fee to suspend or revoke e-MARC Certificates.

2.5.2 Certificate Access Fees

The Authorized CA shall not impose any certificate access fees on Subscribers with respect to its own e-MARC Certificate(s) or the status of such e-MARC Certificate(s).

2.5.3 Revocation Status Information Access Fees (Certificate Validation Services)

Fees may be assessed for certificate validation services as set forth in the Authorized CA's e-MARC Contract. Validation services shall include both Online Certificate Status Protocol (OCSP) Responders and Certificate Revocation Lists (CRL).

2.5.4 Fees for Other Services such as Policy Information

The authorized CA shall not impose fees for access to policy information.

2.5.5 Refund Policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Information

Each Authorized CA shall operate a secure online Repository available to Subscribers and Qualified Relying Parties that shall contain: (1) all e-MARC Certificates issued by the Authorized CA that have been accepted by the Subscriber; (2) a Certificate Revocation List ("CRL") and online certificate status information; (3) the Authorized CA's e-MARC Certificate for its signing key; (4) past and current versions of the Authorized CA's e-MARC CPS; (5) a copy of this Policy; and (6) other relevant information about e-MARC Certificates.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the Authorized CA. The Subscriber will publish e-MARC Certificates issued by the Authorized CA promptly upon acceptance of such e-MARC Certificates. Information relating to the status of an e-MARC Certificate will be published in accordance with the Authorized CA's NERC e-MARC Contract.

2.6.3 Access Controls

The Authorized CA shall not impose any access controls on this Policy, the Authorized CA's e-MARC Certificate for its signing key, and past and current versions of the Authorized CA's e-MARC CPS. The Authorized CA may impose access controls on e-MARC Certificates and e-MARC Certificate status information, in accordance with provisions of the Authorized CA's e-MARC Contract.

2.6.4 Repositories

See Section 2.6.1.

2.7 QUALITY ASSURANCE INSPECTION AND REVIEW

The Authorized CA, including all of its RA, CMA, and Repository subcontractor(s), shall undergo e-MARC Security Certification and Accreditation ("C&A") as a condition of obtaining and retaining approval to operate as an Authorized CA under this Policy and e-MARC Contract. The purpose of the C&A process shall be to verify that the CA has in place and follows a system that assures that the quality of its Authorized CA Services conforms to the requirements of this Policy and the e-MARC Contract.

2.7.1 Frequency of Certification Authority Compliance Review

Certification authorities shall undergo C&A from the Policy Authority prior to initial approval as an Authorized CA, to demonstrate compliance with this Policy, their e-MARC CPS, and e-MARC contracts. Re-certification may be required every 12 months or at any time that a significant change in their operations is made, whichever occurs first, to demonstrate continuing compliance.

2.7.2 Identity/Qualifications of Reviewer

An independent security audit firm acceptable to the Policy Authority that is qualified to perform a security

audit on a CA shall conduct the C&A process.

2.7.3 Auditor's Relationship to Audited Party

No stipulation.

2.7.4 Topics Covered by Quality Assurance Inspection and Review

The C&A quality assurance inspection shall be conducted pursuant to the guidance provided in the American Institute of Certified Public Accountants' / Canadian Institute of Chartered Accountants (AICPA/CICA's) WebTrust Principles and Criteria for Certification Authorities or their equivalent.

2.7.5 Actions Taken as a Result of Deficiency

The Policy Authority will address any identified deficiencies with the e-MARC CA.

2.7.6 Communication of Results

Results of the C&A review will be made available to the Policy Authority, to be used in determining the CA's suitability for initial and continued performance as an Authorized CA.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to Be Kept Confidential

Subscriber Information. The Authorized CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, e-MARC Certificate application, authentication, and certificate status checking processes in accordance with the *Privacy Act of 1974*. Such information shall be used only for the purpose of providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC Contract, and shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the Authorized CA Services in accordance with the e-MARC Contract. In addition, personal information submitted by Subscribers:

(a) must be made available by the Authorized CA to the Subscriber involved following an appropriate request by such Subscriber;

(b) must be subject to correction and/or revision by such Subscriber;

(c) must be protected by the Authorized CA in a manner designed to ensure the data's integrity; and

(d) cannot be used or disclosed by the Authorized CA for purposes other than the direct operational support of e-MARC unless such use is authorized by the Subscriber involved.

Under no circumstances shall the Authorized CA (or any authorized RA, CMA, or Repository) have access to the private keys of any Subscriber to whom it issues an e-MARC Certificate.

Other Subscriber Information. The Authorized CA shall take reasonable steps to protect the confidentiality of Qualified Relying Party, or other Subscriber information provided to the Authorized CA. Such information shall be used only for the purpose of providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC Contract, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the Authorized CA Services in accordance with the e-MARC contract.

2.8.2 Types of Information Not Considered Confidential

Information contained on a single e-MARC Certificate or related status information shall not be considered confidential, when the information is used in accordance with the purposes of providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC contract and in accordance with the *Privacy Act of 1974*. However, a compilation of such information shall be treated as confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See 2.8.2.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discover

No stipulation.

2.8.6 Disclosure upon Owner's Request

See 2.8.1.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in an e-MARC Certificate. This Policy is the property of the Policy Authority. "Energy Market Access and Reliability Certificates," "e-MARC", and the e-MARC OIDs are the property of the Policy Authority, which may be used only by Authorized CAs in accordance with the provisions of this Policy and the Authorized CA's e-MARC Contract. Any other use of the above without the express written permission of the Policy Authority is expressly prohibited.

Section 3

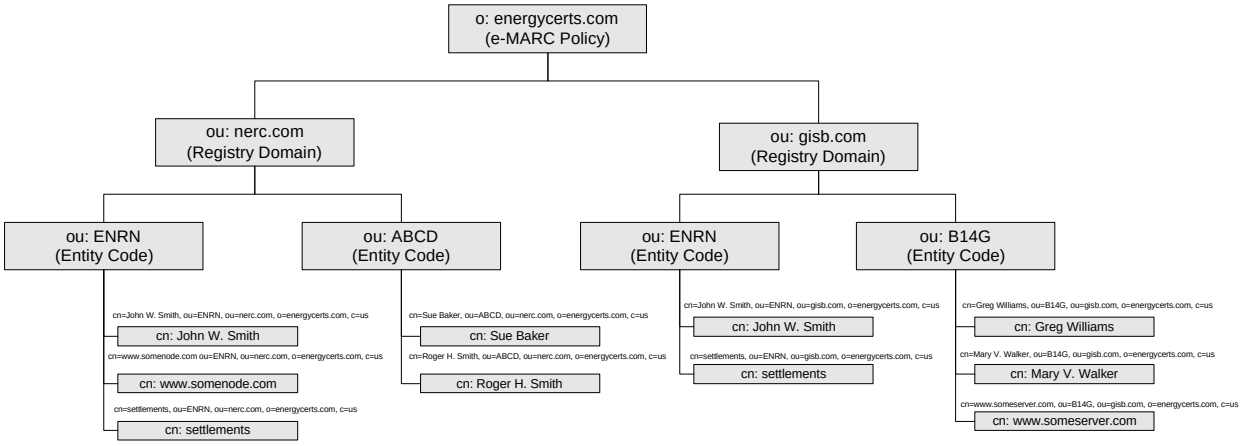
Identification And Authentication

3.1 INITIAL REGISTRATION

Subject to the requirements noted below, applications for e-MARC Certificates may be communicated from the applicant to an Authorized CA or an authorized RA, and authorizations to issue e-MARC Certificates may be communicated from an authorized RA to an Authorized CA, (1) electronically, provided that all communication is secure, (2) by postal mail , or (3) in person. The applicant must also specify in their application, which Registry Domain they are requesting a certificate under and include their unique "Entity Code" assigned to them by the Registry. Unaffiliated individuals, however, do not have to provide an "Entity Code."

3.1.1 Types of Names

All e-MARC Certificates shall contain a unique X.500 Distinguished Name (DN) that must be a printable string, must not be blank, and in the case of a Qualified Relying Party, Business Representative or Device certificate, must clearly and uniquely identify the Registry Domain and the Entity Code of the organization in the Registry Domain as shown in the ***example*** below.



3.1.2 Name Meanings

In the case of Unaffiliated Individuals, the authenticated common name should be a combination of first name, surname and an optional middle initial. In the case of Business Representatives, the authenticated common name should be the combination of first name, surname and an optional middle initial. In the case of Qualified Relying Parties, the authenticated common name should be the combination of first name, surname and an optional middle initial.

Where a certificate refers to a role or position, the certificate must also contain the name of a person who holds that role or position and is responsible for the certificate in the altSubject field of the certificate.

A certificate issued for a device or application must include within the DN the name of the person who is responsible for that device or application in the altSubject field of the certificate.

For Business Representatives, Qualified Relying Parties, and Devices, the DN within the certificate must also contain the Registry Domain and Entity Code of the organization being represented.

3.1.3 Rules for Interpreting Various Name Forms

Not yet defined.

3.1.4 Name Uniqueness

Name uniqueness across all e-MARC Certificates must be enforced and the CA shall enforce name uniqueness within the X.500 name space that they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across all active e-MARC Certificates is ensured. A CA shall document in its CPS what name forms will be used and how they will allocate names within the subscriber community to guarantee name uniqueness among current and past subscribers (i.e., if "Joe Smith" leaves a CA's community of subscribers, and a new, different "Joe Smith" enters the community of subscribers, how will these two individuals be provided unique names). The Registry Domain and Entity Codes contained with an e-MARC Certificate DN shall be provided and maintained by the Registry Administrator.

3.1.5 Name Claim Dispute Resolution Procedures

The CA shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, the CA shall coordinate with and defer to the appropriate naming authority or Registry Administrator but the CA reserves the right to make all final decisions.

3.1.6 Recognition, Authentication, and Role of Trademarks

The use of trademarks will be reserved to registered trademark holders.

3.1.7 Verification of Possession of Key Pair

The Authorized CA shall verify that the applicant possesses the private key corresponding to the public key submitted with the application by utilizing a key transfer protocol or equivalent methods.

3.1.8 Authentication of Sponsoring Organization Identity

If the applicant is requesting a Business Representative e-MARC Certificate, in addition to verifying the applicant's individual identity, as outlined in section 3.1.9, and authorization to represent the Sponsoring Organization, the Authorized CA shall also verify that the Sponsoring Organization exists, is registered

with a unique Entity Code in an approved Registry Domain, and conducts business at the address listed in the e-MARC Certificate application. In conducting its review and investigation, the Authorized CA shall provide validation of information concerning the Sponsoring Organization, including legal company name, type of entity, year of formation, names of directors and officers, address (number and street, city, ZIP code), and telephone number.

If the Sponsoring Organization had previously established the identity of the organization using a process that satisfies the CA and this Policy, and there have been no changes in the information presented, then the CA or RA and the prospective Subscriber may utilize private shared information in order to verify the identity of the Sponsoring Organization.

3.1.9 Authentication of Individual Identity

3.1.9.1 Unaffiliated Individual e-MARC Certificates

Unaffiliated Individuals may be authenticated through an electronically submitted application or by personal presence. In accordance with the e-MARC Contract requirements the Authorized CA shall verify all of the following identification information supplied by the applicant: first name, middle initial, and last name, , current address (number and street, city, ZIP code), and telephone number. Subscriber identification must be confirmed via a NERC-approved identity-proofing process that incorporates the following factors:

a) Submission by the applicant of at least three individual identity items, which must be verified through reference to multiple independent data sources along with cross-checks for consistency, for example:

- Currently-valid credit card number;
- Alien Registration Number;
- Passport number;
- Current employer name, address (number and street, city, ZIP code), and telephone number;
- Currently valid state-issued driver's license number or state-issued identification card number; and
- Social Security Number
- date of birth
- place of birth.

b) At least one of the above data sources must be based on an antecedent in-person or the equivalent identity verification process;

c) The use of an out-of-band notification process that is linked to the requesting individual's physical U.S. postal mail address; or equivalent, and

Verification that the information contained in the Certificate Application is correct.

3.1.9.2 Business Representative and Device e-MARC Certificates

If the applicant is requesting a certificate for a Business Representative, device, or application, the Authorized CA shall verify:

(a) that the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association; and

(b) the Sponsoring Organization's identity as specified in section 3.1.8.

3.1.9.3 Qualified Relying Party e-MARC Certificates

If the applicant is requesting a Qualified Relying Party e-MARC Certificate, The Authorized CA shall verify:

(a) that the applicant is authorized to act on behalf of the Qualified Relying Party;
(b) the affiliation of the e-MARC Certificate applicant with the Qualified Relying Party; and
(c) The Sponsoring Organization's identity as specified in section 3.1.8

3.2 ROUTINE REKEY (RENEWAL)

In accordance with the e-MARC contract the Authorized CA shall accept e-MARC Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the e-MARC Certificate, provided the e-MARC Certificate is not revoked, suspended, or expired. e-MARC Certificates shall be renewed in 1-year increments. In the event that subject information and/or the key pair change, the Authorized CA shall require the Subscriber to request a new e-MARC Certificate. The Authorized CA shall renew e-MARC Certificates issued to Qualified Relying Parties only after completing successful identity proofing verification in accordance with the requirements for identity proofing specified in Section 3.1.9

3.3 REKEY AFTER REVOCATION

In accordance with the e-MARC Contract, suspended, revoked, or expired e-MARC Certificates shall not be renewed. Applicants without a valid e-MARC Certificate shall be re-authenticated by the Authorized CA or an authorized RA through a new e-MARC Certificate application, just as with an initial applicant registration, and shall be issued a new e-MARC Certificate.

3.4 REVOCATION REQUEST

In accordance with the e-MARC contract and section 4.4.1, an e-MARC Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the e-MARC Certificate's associated key pair. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 3. Revocation requests authenticated on the basis of the e-MARC Certificate's associated key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via postal mail, or equivalent. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

Section 4

Operational Requirements

4.1 CERTIFICATE APPLICATION

Application Initiation. The following persons may initiate the e-MARC Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative, device, or application	Sponsoring Organization; or potential Subscriber
Qualified Relying Party	Duly authorized representative of the Qualified Relying Party

(a) Application Form. An applicant for an e-MARC Certificate shall complete an e-MARC Certificate application and provide requested information in a form prescribed by the Authorized CA and this Policy.

(b) Applicant Education and Disclosure. At the time of e-MARC Certificate application, the Authorized CA shall inform applicants of the advantages and potential risks associated with using e-MARC Certificates to access Qualified Relying Parties electronically and provide information to Subscribers regarding the use of private keys and digital signatures created with such keys, and Subscriber obligations.

4.2 CERTIFICATE ISSUANCE

Upon successful completion of the Subscriber identification and authentication process in accordance with the e-MARC contract, the Authorized CA shall create the requested e-MARC Certificate, notify the applicant thereof, and make the e-MARC Certificate available to the applicant. The Authorized CA shall use an out-of-band notification process linked to the e-MARC Certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the e-MARC Certificate only to the Subscriber. Upon issuance of an e-MARC Certificate, the Authorized CA warrants to all Program Participants that:

(a) The Authorized CA has issued, and will manage, the e-MARC Certificate in accordance with the requirements in this Policy;
(b) The Authorized CA has complied with all requirements in this Policy when identifying the Subscriber and issuing the e-MARC Certificate;
(c) There are no misrepresentations of fact in the e-MARC Certificate known to the Authorized CA and the Authorized CA has verified the information in the e-MARC Certificate;
(d) Information provided by the Subscriber for inclusion in the e-MARC Certificate has been accurately transcribed to the e-MARC Certificate; and
(e) The e-MARC Certificate meets the material requirements of this Policy.

4.3 CERTIFICATE ACCEPTANCE

As described in the e-MARC contract a condition to issuing the e-MARC Certificate, the Subscriber shall

indicate acceptance or rejection of the e-MARC Certificate to the Authorized CA and acknowledge the Subscriber obligations under Section 2.1.5. By accepting the e-MARC Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the e-MARC Certificate are true.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Who Can Request Revocation

The only persons permitted to request revocation of an e-MARC Certificate issued pursuant to this Policy are the Subscriber, the Sponsoring Organization (where applicable), the Registry Administrator (where applicable), and the issuing Authorized CA.

4.4.2 Circumstances for Revocation

4.4.2.1 Permissive Revocation

As described in the e-MARC contract a Subscriber may request revocation of his/her/its e-MARC Certificate at any time for any reason. A Sponsoring Organization may request revocation of an e-MARC Certificate issued to its Business Representative (device or individual) at any time for any reason.

4.4.2.2 Required Revocation

A Subscriber, a Sponsoring Organization (where applicable), or a Registry Administrator (where applicable) is responsible for promptly requesting revocation of an e-MARC Certificate:

(a) When any of the information on the e-MARC Certificate changes or becomes obsolete;

(b) When the private key, or the media holding the private key, associated with the e-MARC Certificate is, or is suspected of having been, compromised;

(c) When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization;

(d) When a device or server is no longer active or no longer affiliated with a Sponsoring Organization.

(e) Upon a change of an Individual or Sponsoring Organization's registration in the Registry Domain (where applicable). Changes in registration include DUNS number or Entity Code, or any other attribute that the appropriate Registry Administrators deems to warrant revocation and is in accordance with the policy.

(d) If an Authorized CA learns, or reasonably suspects, that the Subscriber's private key has been compromised; or

(e) If the issuing Authorized CA determines that the e-MARC Certificate was not properly issued in accordance with this Policy and/or the Authorized CA's e-MARC CPS.

Failure to do so is at the subscriber's risk.

4.4.3 Procedure for Revocation Request

As described in the e-MARC Contract an e-MARC Certificate revocation request should be promptly communicated to the issuing Authorized CA, either directly or through the RA authorized to accept such notices on behalf of the Authorized CA. An e-MARC Certificate revocation request may be communicated electronically if it is digitally signed with the private key of the Subscriber, the Sponsoring Organization (where applicable), or Registry Administrator (where applicable). Alternatively, the Subscriber, Sponsoring Organization (where applicable), or Registry Administrator (where applicable) may request revocation by contacting the issuing Authorized CA or its RA in person and providing adequate proof of identification in accordance with this Policy.

4.4.4 Revocation Request Grace Period

Revocation is immediate if the certificate has been compromised. A 2 week (10 business days) grace period may be given in all other situations, at the CA's discretion.

4.4.5 Circumstances for Suspension

A certificate **may** be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request.

4.4.6 Who Can Request Suspension

See Section 4.4.1.

4.4.7 Procedure for Suspension Request

See Section 4.4.3.

4.4.8 Limits on Suspension Period

Not yet defined.

4.4.9 CRL Issuance Frequency

A CA must ensure that it issues an up to date CRL at least every twelve hours. A CA must ensure that its CRL issuance is synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to Qualified Relying Parties. When a certificate is revoked due to a key compromise, the updated CRL must be issued immediately.

4.4.10 OCSP/CRL Checking Requirements

A Qualified Relying Party must check the status of all certificates in the certificate validation chain against

an Online Certificate Status Protocol (OCSP) responder, or the current CRL prior to their use. If using a CRL, the Qualified Relying Party must also verify the authenticity and integrity of CRLs.

4.4.11 Online Revocation/Status Checking Availability

Authorized CAs shall validate online, near real-time, the status of the e-MARC Certificate indicated in an e-MARC Certificate validation request message (via OCSP).

4.4.12 Online Revocation Checking Requirements

Each Qualified Relying Party will validate every e-MARC Certificate it receives in connection with a transaction. A transaction may be considered any financially binding or data manipulating action as determined by the software application or process being implemented.

4.4.13 Other Forms of Revocation Advertisements Available

Not yet defined.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

Not yet defined.

4.4.15 Special Requirements re: Key Compromise

In the event of the compromise, or suspected compromise, of a CA signing key, the CA must immediately notify the Policy Authority and all CAs to whom it has issued cross-certificates.

In the event of the compromise, or suspected compromise, of any other Entity's signing key, an Entity must notify the issuing CA immediately.

A CA must ensure that its CPS or publicly available documents and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.5 COMPUTER SECURITY AUDIT PROCEDURES

All significant security events on each Authorized CA's system shall be automatically recorded in audit trail files. Such files shall be securely archived in accordance with Section 4.6.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Recorded

The data and files which must be archived by or on behalf of each Authorized CA include:

- e-MARC certificate application information;
- certificate issuance and transaction data;

- system start-up and shutdown;
- CA application start-up and shutdown;
- Attempts to create, remove, set passwords or change the system privileges of the PKI Master Office, PKI Office, or PKI Administrator;
- Changes to CA details and/or keys;
- Changes to certificate creation policies e.g., validity period;
- Login and logoff attempts;
- Unauthorized attempts at network access to the CA system;
- Unauthorized attempts to access system files;
- Generation of own and subordinate Entity keys;
- Revocation of certificates;
- Attempts to initialize, remove, enable, and disable Subscribers, and update and recover their keys;
- Failed read-and-write operations on the certificate and CRL directory.

All logs, whether electronic or manual, should contain the date and time of the event, and the identity of the entity which caused the event.

A CA should also collect and consolidate, either electronically or manually, security information not CA-System generated such as:

- Physical access logs;
- System configuration changes and maintenance;
- Personnel changes;
- Discrepancy and compromise reports;
- Record of the destructions of media containing key material, activation data, or personal Subscriber information.

A CA must ensure that all significant logged events are explained in an audit log summary and that audit logs are actively reviewed either manually or automatically on a regular basis. Actions taken following these reviews must be documented.

4.6.2 Retention Period for Archive

No stipulation.

4.6.3 Protection of Archive

The archive media must be protected at least at the level required to maintain and protect all Subscriber information and data from disclosure, modification, or destruction.

4.7 KEY CHANGEOVER

A Subscriber may only apply to renew his or her key pair within three months prior to the expiration of the keys, provided the certificate has not been revoked. A Subscriber or the CA may initiate this key changeover process and automated key changeover is permitted. Subscribers without valid keys must be re-authenticated by the CA or LRA in the same manner as the initial registration. In the case of Business Representatives, devices, or applications, the CA must verify that the Business Representative, device, or

application is still an authorized representative of the Sponsoring Organization prior to a key changeover.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing Resources, Software, and/or Data are corrupted

The CA must establish business procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where a repository is not under the control of the CA, a CA must ensure any agreement with the repository provides that business continuity procedures be established and documented by the repository.

4.8.2 Authorized CA Public Key Is Revoked

In the even of the need for revocation of a CA's Digital Signature certificate, the CA must immediately notify:

- The Policy Authority;
- All CAs to whom it has issued cross-certificates;
- All of its RAs;
- All Subscribers;
- All individuals or organizations who are responsible for a certificate used by a device or application.

The CA must also:

- Publish the certificate serial number on an appropriate CRL;
- Revoke all cross-certificates signed with the revoked Digital Signature certificate.

After addressing the factors that led to revocation, the CA may:

- Generate a new CA signing key pair;
- Re-issue certificates to all Subscribers and ensure all CRLs are signed using the new key.

4.8.3 Authorized CA Private Key Is Compromised (*Key Compromise Plan*)

As required by the e-MARC contract each Authorized CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by an Authorized CA to issue e-MARC Certificates. Such plan shall include procedures for revoking all affected e-MARC Certificates and promptly notifying all Subscribers and all Qualified Relying Parties.

4.8.4 Secure Facility after a Natural or Other Disaster (*Disaster Recovery Plan*)

An Authorized CA must have in place an appropriate disaster recovery/business resumption plan. Such plan shall be detailed within the Authorized CA's e-MARC CPS. or other appropriate documentation made available to and approved by the Policy Authority.

4.9 AUTHORIZED CA CESSATION OF SERVICES

In the event that an Authorized CA ceases operation or its participation as an Authorized CA in e-MARC or is otherwise terminated,

(a) all Subscribers, sponsoring organizations, and Qualified Relying Parties must be promptly notified of the cessation;
(b) all e-MARC Certificates issued by an Authorized CA shall be revoked no later than the time of cessation; and
(c) all current and archived e-MARC identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to Policy Authority within 24 hours of cessation and in accordance with this Policy. Transferred data shall not include any non-e-MARC data.

If the CA has arranged for the transfer and retention of the CA's keys and information to another CA that meets the requirements of this policy and the Policy Authority, service may be continued under the new CA and certificates need not be revoked.

4.10 CUSTOMER SERVICE CENTER

As described in the e-MARC contract each Authorized CA shall implement and maintain an e-MARC Customer Service Center to provide assistance and services to Subscribers and Qualified Relying Parties, and a system for receiving, recording, responding to, and reporting e-MARC problems within its own organization and for reporting such problems to the Policy Authority.

Section 5

Physical, Procedural, and Personnel Security Controls

5.1 PHYSICAL SECURITY CONTROLS

Each Authorized CA, and all associated RAs, CMAs, and Repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Authorized CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

A CA should provide for a minimum of two distinct PKI personnel roles, distinguishing between day-to-day operation of the CA system and the management and audit of those operations. The selection and distinction of trusted roles must provide resistance to insider attack.

5.2.2 Number of Persons Required Per Task

An Authorized CA shall utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.

5.2.3 Identification and Authentication for Each Role

All CA personnel must have their identity and authorization verified before they are:

- included in the access list for the CA site;
- included in the access list for physical access to the CA system;
- given a certificate for the performance of their CA role;
- given an account on the PKI system.

Each of these certificates and accounts must:

- be directly attributable to an individual;
- not be shared;
- be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 PERSONNEL SECURITY CONTROLS

Each Authorized CA and its RA, CMA, and Repository subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this Policy.

Section 6

Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(a) General. Key pairs for all Program Participants must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Authorized CA, RA, and CMA keys may be generated in either hardware or software, although hardware based key generations is preferred. Key pairs for Subscribers and Qualified Relying Party application can be generated in either hardware or software.

6.1.2 Private Key Delivery to Entity

See Section 6.1.1.

6.1.3 Subscriber Public Key Delivery to Authorized CA

As part of the e-MARC Certificate application process, the Subscriber's public key must be transferred to the Registration Authority or Authorized CA in a way that ensures that (1) it has not been changed during transit; (2) the sender possesses the private key that corresponds to the transferred public key; and (3) the sender of the public key is the legitimate user claimed in the certificate application. If done on-line, the delivery mechanism should be in accordance with the PKIX-3 Certificate Management Protocol, or via an equally secure manner.

6.1.4 Authorized CA Public Key Delivery to Users

No stipulation.

6.1.5 Key Sizes

Key sizes and algorithms shall be a minimum of 1024 bits and preferably 2048 bits for all e-MARC Certificates.

6.2 AUTHORIZED CA PRIVATE KEY PROTECTION

Each Authorized CA, RA, and CMA shall each protect its private key(s) in accordance with the provisions of their e-MARC contract, this Policy, and best industry practice.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The issuing CA must retain all verification public keys.

6.3.2 Usage Periods for the Public and Private Keys (*Key Replacement*)

Subscriber key pair must be replaced in accordance with the validity periods specified in the applicable certificate profile.

6.3.3 Restrictions on CA's Private Key Use

The private key used by Authorized CAs for issuing e-MARC Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses.

A private key held by a CMA, if any, and used for purposes of manufacturing e-MARC Certificates is considered the Authorized CA's signing key, is held by the CMA as a fiduciary, and shall not be used by the CMA for any other purposes, except as agreed by NERC and the Authorized CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

The private key used by each RA employed by an Authorized CA in connection with the issuance of e-MARC Certificates shall be used only for communications relating to the approval or revocation of such certificates.

6.4 ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

No stipulation.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulation.

Section 7

Certificate and CRL Profiles

7.1 CERTIFICATE PROFILE

e-MARC Certificates shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification and symmetric key exchange.

The Authorized CA shall create and maintain e-MARC Certificates that conform to the ITU-T Recommendation X.509, "The Directory: Authentication Framework," June 1997.
All e-MARC Certificates must include a reference to an OID for this Policy within the appropriate field, and contain the required certificate fields according to the Authorized CA's CPS and the e-MARC Contract.

7.2 CRL PROFILE

No stipulation.

Section 8

Policy Administration

8.1 POLICY CHANGE PROCEDURES

8.1.1 List of Items

Notice of all proposed changes to this Policy under consideration by the Policy Authority that may materially affect users of this Policy (other than editorial or typographical corrections, changes to the contact details, or other minor changes) will be provided to Authorized CAs, subscribers, and Qualified Relying Parties, and will be posted on the Policy Authority World Wide Website. The Authorized CA shall post notice of such proposed changes and shall advise their Subscribers of such proposed changes.

8.1.2 Comment Period

Any interested person may file comments with the Policy Authority within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

A copy of this Policy is available in electronic form on the Internet and via e-mail from the Policy Authority. The Authorized CA shall also make available copies of this Policy both online and in hard copy form.

8.3 CPS APPROVAL PROCEDURES

The Policy Authority must approve an Authorized CA's e-MARC CPS prior to its incorporation into the Authorized CA's operational procedures.

Glossary

e-MARC. Energy Market Access and Reliability Certificates. Aimed at providing commercial public key certificate services to the those participating in energy markets and identified in authorized Registry Domains.

e-MARC Certificates. Certificates issued by an Authorized CA in accordance with this Policy, which certificates reference, this Policy by inclusion of the e-MARC OID.

e-MARC CPS. An e-MARC CPS is a certification practice statement of the practices that an Authorized CA employs in issuing, suspending, and revoking e-MARC Certificates and providing access to the same.

Agency. A term used to identify all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, and, when authorized by law or regulation, state, local, and tribal Governments.

Agency Applications. See "Qualified Relying Party."

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Authorized CA. A certification authority that has been authorized by the Policy Authority to issue e-MARC Certificates and provide Authorized CA Services under the Policy.

Authorized CA Services. The services relating to e-MARC Certificates to be provided by Authorized CAs under this Policy (See section 2.1.1).

CA. See "certification authority."

Certificate. A data record that, at a minimum: (a) identifies the Authorized CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a public key that corresponds to a private key under the control of the Subscriber; (d) identifies its operational period; and (e) contains an e-MARC Certificate serial number and is digitally signed by the Authorized CA issuing it. As used in this Policy, the term of "Certificate" refers to certificates that expressly reference the OID of this Policy in the "*CertificatePolicies*" field of an X.509 v.3 certificate.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of e-MARC Certificates signed by an Authorized CA, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is an entity that is delegated or outsourced the task of actually manufacturing the Certificate on behalf of an Authorized CA).

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. See "Authorized CA."

Certification Practice Statement. A "certification practice statement" is a statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing certificates and providing access to same, in accordance with specific requirements (i.e., requirements specified in this Policy, requirements specified in a contract for services).

CMA. See "Certificate Manufacturing Authority".

CPS. See "Certification Practice Statement".

CRL. Certificate Revocation List

CSOR. Computer Security Objects Register operated by the National Institute of Standards and Technology.

Digital Signature. A digital signature is a string of bits associated with a collection of data (e.g., a file, document, message, transaction); this string of bits can only be generated by the holder of a private key, but can be verified by anyone with access to the corresponding public key. Note that some algorithms include additional steps (e.g., one-way hashes, timestamps) in this basic process.

DSA. Digital Signature Algorithm

DSS. Digital Signature Standard

Entity Code. A unique alphanumeric code assigned to a registered organization in a Registry Domain by the Registry Administrator.

FAR. Federal Acquisition Regulation

FED-STD. Federal Standard

FIPS. Federal Information Processing Standards. These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

FIPS PUB Federal Information Processing Standards Publication

Government. Federal Government and authorized agencies and entities.

NERC. North America Electric Reliability Counsel

e-MARC Contract.

e-MARC Operating Agreement.

IETF. See "Internet Engineering Task Force."

Internet Engineering Task Force (IETF). The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

ISO. International Standards Organization

ITU. International Telecommunications Union

ITU-T. International Telecommunications Union – Telecommunications Sector

ITU-TSS. International Telecommunications Union – Telecommunications Systems Sector

Key Changeover (CA). The procedure used by a Authorities to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

Key pair. Means two mathematically related keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authentication).

NIST. National Institute of Standards and Technology.

Object Identifier. An object identifier is a specially formatted number that is registered with an internationally-recognized standards organization.

OID. See "Object Identifier".

Operating Rules. See "e-MARC Operating Rules".

Operational Period of an e-MARC Certificate. The operational period of an e-MARC Certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

Out-of-band. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party using U.S. Postal mail to communicate with another party where current communication is online communication).

PKI. Public Key Infrastructure

PIN. Personal Identification Number

Policy. Means this Certificate Policy.

Policy Authority. The entity specified in Section 1.4

Private Key. The key of a key pair used to create a digital signature. This key must be kept a secret.

Program Participants. Collectively, the Registry Administrators, Authorized CAs, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified Relying Parties, and Policy Authority authorized to participate in the public key infrastructure defined by this Policy.

Public Key. The key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via an e-MARC Certificate issued by an Authorized CA and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

Qualified Relying Party. A recipient of a communication event protected by a certificate-based security service that is authorized by this Policy to rely on an e-MARC Certificate to verify the digital signature on the message, including the revocation status of any presented certificate.

RA. See "Registration Authority."

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an Authorized CA)

Registry Domain. A registry of market participant. A Registry Domain typically describes a bounded set of market participants within a particular energy segment, such as gas or electricity. The Registry and Registry Domain must comply with the policies set forth in this document and have a unique registered Internet domain name.

Registry Administrator. An entity or organization authorized to administer a Registry Domain in accordance with the policies set forth in this document.

Repository. A database containing information and data relating to certificates, and an Authorized CA, as specified in this Policy.

Responsible Individual. A trustworthy person designated by a Sponsoring Organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. Means to prematurely end the operational period of a Certificate from a specified time forward.

Sponsoring Organization. A business entity, government agency, or other organization with which a Business Representative is affiliated (e.g., as an employee, agent, member, user of a service, business partner, customer, etc.).

Subject. A person whose public key is certified in an e-MARC Certificate. Also referred to as a "Subscriber".

Subscriber. A Subscriber is a person who (1) is the subject named or identified in an e-MARC Certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a Certificate. Means to temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.

Transaction. Any financially binding action. As defined by the software application or process being secured or implemented.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

U.S.C. United States Code

Valid Certificate. Means an e-MARC Certificate that (1) an Authorized CA has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, an e-MARC Certificate is not "valid" until it is both issued by an Authorized CA and has been accepted by the Subscriber.

WWW. World Wide Web