Smart Grid Standards Information

Version 1.7
Wednesday, May 19, 2010

Section I: Use and Application of the Standard

A. Identification and Affiliation

1.	Number of the standard	62351
2.	Title of the standard	Parts 1-8, Information Security for Power System Control Operations
3.	Name of owner organization	International Electrotechnical Commission (IEC)
4.	Latest versions, stages, dates	• IEC/TS 62351-1 ed1.0 (2007-05): Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues • IEC/TS 62351-2 ed1.0 (2008-08): Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms • IEC/TS 62351-3 ed1.0 (2007-06): Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP • IEC/TS 62351-4 ed1.0 (2007-06): Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS • IEC/TS 62351-5 ed1.0 (2009-08): Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives • IEC/TS 62351-6 ed1.0 (2007-06): Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850 • IEC/TS 62351-7 TS Ed.1 (2008-04): Power systems management and associated information exchange - Data and communication security - Part 7: Network and system management (NSM) data object models • IEC/TS 62351-8 Ed. 1.0 (ACDV — Draft approved for Committee Draft with Vote): Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control

Section I: Use and Application of the Standard

5.	URL(s) for the standard	• IEC/TS 62351-1 ed1.0 (2007-05): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/37996 • IEC/TS 62351-2 ed1.0 (2008-08): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/41812 • IEC/TS 62351-3 ed1.0 (2007-06): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/38093 • IEC/TS 62351-4 ed1.0 (2007-06): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/38094 • IEC/TS 62351-5 ed1.0 (2009-08): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/43284 • IEC/TS 62351-6 ed1.0 (2007-06): http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/38092 • IEC/TS 62351-7 TS Ed.1 (2008-04): http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=62351&Pa=7&Se=&Am=&Fr=&TR=TS&Ed=1 • IEC/TS 62351-8 Ed. 1.0: http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=62351&Pa=8&Se=&Am=&Fr=&TR=TS&Ed=1
6.	Working group / committee	TC57
7.	Original source of the content (if applicable)	
8.	Brief description of scope	IEC 62351 Parts 1-8, Information Security for Power System Control Operations, define security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation and protection.

B. Level of Standardization

1.	Names of standards development organizations that recognize this standard and/or accredit the owner organization	All
2.	Has this standard been adopted in regulation or legislation, or is it under consideration for adoption?	☐ Yes ☒ No
3.	Has it been endorsed or recommended by any level of government? If "Yes", please describe	☐ Yes ☒ No
4.	Level of Standard (check all that apply)	☒International ☐National ☐Industry ☐de Facto ☐ Single Company
5.	Type of document	☒Standard ☐ Report ☐ Guide ☐ Technical Specification
6.	Level of Release	☒ Released ☐ In Development ☐ Proposed

Section I: Use and Application of the Standard

C. Areas of Use

1.	Currently used in which domains? (check all that apply)	□ Markets ☒ Operations □ Service Providers ☒ Generation ☒ Transmission ☒ Distribution □ Customer
2.	Planned for use in which domains? (check all that apply)	□ Markets ☒ Operations ☒Service Providers ☒ Generation ☒ Transmission ☒ Distribution ☒ Customer
3.	Please describe the Smart Grid systems and equipment to which this standard is applied	All interactions among systems and equipment which use protocols and message exchanges based on IEC TC57 standards, including IEC 61850 (substation automation, hydro plants, distribution automation, and distributed energy resources), 61968 (CIM for distribution), 61970 (CIM for transmission), 60870-5, 60870-6 (ICCP), and DNP3 (as a derivative of 60870-5). Where applicable in the future, these standards will apply to PEVs and HAN interactions.

Section I: Use and Application of the Standard		
D. Relationship to Other Standards or Specifications		
1.	Which standards or specifications are referenced by this standard?	• RFC 2246:1999, The TLS Protocol Version 1.01) • RFC 2712:1999, Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)2) • RFC 3268, 2002, Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS) • RFC 3280, 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate • Revocation List (CRL) Profile • ISO 9506 – Manufacturing Message Specification (MMS) • ISO/IEC 9798-4, Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function • FIPS 186-2, Digital Signature Standard (DSS) • FIPS 197, Advanced Encryption Standard (AES) • FIPS 198-1, The Keyed-Hash Message Authentication Code • RFC 2104, HMAC: Keyed-Hashing for Message Authentication • RFC 3174, Secure Hash Algorithm (SHA-1) • RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm • RFC 3629, UTF-8, a transformation format of ISO 10646 • RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI • RFC 2313, PKCS #1: RSA Encryption Version 1.5 • RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, Version 2.1 • RFC 4634, US Secure Hash Algorithms (SHA and HMAC-SHA) • ANSI INCITS 359-2004: Role Based Access Control • PKCS#12: Personal Information Exchange Syntax Standard • ISO 9594-8/ITU-T Rec. X.509 (2005) The Directory: Public-key and attribute certificate frameworks • IEC 62400: Structuring principles for technical products and technical product documentation - Letter codes - Main classes and subclasses of objects according to their purpose and task
2.	Which standards or specifications are related to this standard?	IEC 61850 (substation automation, hydro plants, distribution automation, and distributed energy resources), 61968 (CIM for distribution), 61970 (CIM for transmission), 60870-5, 60870-6 (ICCP), and DNP3 (as a derivative of 60870-5). Where applicable in the future, these standards will apply to PEVs and HAN interactions.
3.	Which standards or specifications cover similar areas (may overlap)?	No specific overlaps, but are built on refinements and constraints of other standards
4.	What activities are building on this work?	All activities involving the IEC TC57 protocols

Section I: Use and Application of the Standard

E. Dept of Energy Smart Grid Characteristics

Please describe how this standard may encourage each of the following:

1.	Enables informed participation by customers	□ Yes □ No
2.	Accommodates all generation and storage options	☒ Yes □ No
3.	Enables new products, services and markets	☒ Yes □ No
4.	Provides the power quality for a range of needs	□ Yes □ No
5.	Optimizes asset utilization and operating efficiency	□ Yes □ No
6.	Operates resiliently to disturbances, attacks, and natural disasters	☒ Yes □ No

F. Priority Areas Previously Mentioned by FERC and NIST

Please describe if and how this standard may be applied in each of the following areas. Note that there is space in section J to discuss any other significant areas where the standard may be applied.

1.	Cybersecurity and physical security	☒ Yes ☐ No
2.	Communicating and coordinating across inter-system interfaces	☒ Yes ☐ No
3.	Wide area situational awareness	☒ Yes ☐ No
4.	Smart grid-enabled response for energy demand	☒ Yes ☐ No
5.	Electric storage	☒ Yes ☐ No
6.	Electric vehicle transportation	☒ Yes ☐ No
7.	Advanced metering infrastructure	☒ Yes ☐ No
8.	Distribution grid management	☒ Yes ☐ No

G. Openness

1.	Amount of fee (if any) for the documentation	Yes, see IEC web site
2.	Amount of fee (if any) for implementing the standard	No
3.	Amount of fee (if any) to participate in updating the standard	No
4.	Is the standard documentation available online?	☒ Yes □ No URL: www.iec.ch
5.	Are there open-source or reference implementations?	□ Yes ☒ No
6.	Are there open-source test tools?	□ Yes ☒ No
7.	Would open-source implementations be permitted?	☒ Yes □ No
8.	Approximately how many implementers are there?	Mostly implemented by power system control system vendors who incorporate these cyber security standards into their products
9.	Approximately how many users are there?	Utilities who have purchased systems from vendors who have incorporated the standards
10.	Where is the standard used outside of the USA?	Europe, Asia, South America
11.	Is the standard free of references to patented technology?	☒ Yes □ No
12.	If patented technology is used, does the holder provide a royalty-free license to users of the standard?	□ Yes □ No ☒ Not Patented
13.	Can an implementer use the standard without signing a license agreement?	☒ Yes □ No
14.	Are draft documents available to the public at no cost?	☒ Yes □ No
15.	How does one join the working group or committee that controls the standard?	Ask your IEC National Committee to join IEC TC57 WG15
16.	Is voting used to decide whether to modify the standard? If Yes, explain who is permitted to vote.	☒ Yes □ No IEC National Committees
17.	Is an ANSI-accredited process used to develop the standard?	☒ Yes □ No
18.	What countries are represented in the working group or committee that controls the standard?	USA, Canada, most of Europe, Argentina, Japan, China, etc.

H. Support, Conformance, Certification and Testing

1.	Is there a users group or manufacturers group to support this standard?	☒ Yes □ No
2.	What is the name of the users group or manufacturers group (if any)?	IEEE PES PSCC Security Subcommittee
3.	What type of test procedures are used to test this standard? (please check all that apply)	□ Internal to the lab □ Published by standards organization □ Published by users group ☒ No procedures, informal testing
4.	Are there test vectors (pre-prepared data) used in testing? (please check all that apply)	□ Internal to the lab □ Published by standards organization □ Published by users group ☒ No procedures, informal testing

5.	What types of testing programs exist? (check all that apply)	☐ Interoperability Testing ☐ Conformance Testing ☐ Security Testing ☒ No Testing
6.	What types of certificates are issued? (check all that apply)	☐ Interoperability Certificate ☐ Conformance Certificate ☐ Security Certificate (text document) ☒ No Certificates
7.	Are there rules controlling how and when to use the logo?	☒ Yes ☐ No ☐ Standard has no logo
8.	Is there a program to approve test labs?	☐ Yes ☒ No
9.	Approximately how many test labs are approved (if any)?	
10.	Is there a defined process for users to make technical comments on the standard or propose changes to the standard and have these issues resolved?	☒ Yes ☐ No
11.	Is there a published conformance checklist or table?	☐ Yes ☒ No
12.	Are there defined conformance blocks or subsets?	☒ Yes ☐ No
13.	Approximately how many vendors provide test tools?	A few
14.	Are there tools for pre-certification prior to testing?	☐ Yes ☒ No
15.	Can vendors self-certify their implementations?	☒ Yes ☐ No
16.	Is there application testing for specific uses?	☐ Yes ☐ No ☒ Not applicable
17.	Is there a “golden” or “reference” implementation to test against?	☐ Yes ☒ No
18.	Who typically funds the testing? (check all that apply)	☐ User ☐ Users Group ☒ Vendor ☐ Confidential
19.	Is there a method for users and implementers to ask questions about the standard and have them answered? (check all that apply)	☒ Yes, official interpretations ☒ Yes, informal opinions ☐ No
20.	Does the users’ group (or some other group) fund specific tasks in the evolution of the standard?	☐ Yes ☒ No
21.	Is the users’ group working on integration, harmonization or unification with other similar standards?	☐ Yes ☒ No
22.	What other standards is this standard being integrated, harmonized, or unified with (if any)?	
23.	Are there application notes, implementation agreements, or guidelines available describing specific uses of the standard?	☐ Yes ☒ No ☐ Not applicable

J. Notes

Please present here any additional information about the standard that might be useful:

1. IEC 62351-1 is an introduction to cyber security concepts and terminology, as well as to the 62351 series, thus providing security awareness.

   IEC 62351-2 is a glossary of cyber security terms, and as such has no security requirements. There certainly are security words not covered in the glossary.

   IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 2246) so that they are applicable to the telecontrol environment of IEC TC 57, specifically IEC 61850, 60870-6 (ICCP), and 60870-5 (including DNP3 as a derivative). It covers security for the Network and Transport Layers of the OSI communications stack.

   IEC 62351-4 specifies procedures, protocol extensions, and algorithms to facilitate securing ISO 9506 – Manufacturing Message Specification (MMS)-based applications, specifically IEC 61850 and 60870-6 (ICCP). It covers security for the Application and Transport Layers of the OSI communications stack for MMS.

   IEC 62351-5 specifies messages, procedures and algorithms for securing the operation of all protocols based on or derived from the standard IEC 60870-5, including DNP3. This part of IEC 62351 focuses only on application layer authentication and security issues arising from such authentication, and therefore does not address confidentiality. It provides authentication through challenge/response mechanisms using HMAC and secret key methods, to avoid compute and/or media intensive cryptographic calculations.

   IEC 62351-6 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850, Parts 6, 8-1, and 9-2. It is expected to be used in conjunction (as appropriate) with IEC 62351-3 (TLS) and IEC 62351-4 (MMS).

   IEC 62351-7 covers System and Network Management. Management of the information infrastructure has become crucial to providing the necessary high levels of security and reliability in power system operations. Using the concepts developed in the IETF Simple Network Management Protocol (SNMP) standards for network management, IEC 62351-7 defines Network and System Management (NSM) data object models that are specific to power system operations. These NSM data objects will be used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure.

   IEC 62351-8 addresses Role-Based Access Control (RBAC). The scope of this technical specification is access control of users and automated agents to power system cyber assets by means of role-based access control (RBAC). RBAC is in keeping with the security principle of least privilege, which states that no user should be given more rights than necessary for performing that person’s job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed roles for assignment to specific individuals according to their job needs.

Section II: Functional Description of the Standard

K. GridWise Architecture: Layers

Please identify which layers this standard specifies, as described in http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf, and the applicable section of the standard. Note the mapping to the Open Systems Interconnect (OSI) model is approximate.

1.	**Layer 8: Policy**	□ Yes □ No
2.	**Layer 7: Business Objectives**	☒ Yes □ No
3.	**Layer 6: Business Procedures**	□ Yes □ No
4.	**Layer 5: Business Context**	□ Yes □ No
5.	**Layer 4: Semantic Understanding (object model)**	☒ Yes □ No
6.	**Layer 3: Syntactic Interoperability (OSI layers 5-7)**	☒ Yes □ No
7.	**Layer 2: Network Interoperability (OSI layers 3-4)**	☒ Yes □ No
8.	**Layer 1: Basic Connectivity (OSI layers 1-2)**	☒ Yes □ No

L. GridWise Architecture: Cross-Cutting Issues

Please provide an explanation in the box beside the heading for any questions answered “Not applicable". If the question is not applicable because the function is provided in another layer or standard, please suggest any likely candidates. Note that “the standard” refers to the technology specified by the standard, not the documents themselves.

	Shared Meaning of Content	
1.	Do all implementations share a common information model?	☒ Yes □ No □ Not applicable
2.	Can data be arranged and accessed in groups or structures?	☒ Yes □ No □ Not applicable
3.	Can implementers extend the information model?	☒ Yes □ No □ Not applicable
4.	Can implementers use a subset of the information model?	☒ Yes □ No □ Not applicable
	Resource Identification	
5.	Can data be located using human-readable names?	☒ Yes □ No □ Not applicable
6.	Can names and addresses be centrally managed without human intervention?	□ Yes □ No □ Not applicable
	Time Synchronization and Sequencing	
7.	Can the standard remotely synchronize time?	□ Yes □ No □ Provided in another layer
8.	Can the standard indicate the quality of timestamps?	□ Yes □ No □ Provided in another layer
	Security and Privacy	
9.	Where is security provided for this standard?	☒ Within this standard □ By other standards
10.	Does the standard provide authentication?	☒ Yes □ No
11.	Does the standard permit role-based access control?	☒ Yes □ No

Section II: Functional Description of the Standard

12.	Does the standard provide encryption?	☒ Yes ☐ No
13.	Does the standard detect intrusions or attacks?	☒ Yes ☐ No
14.	Does the standard facilitate logging and auditing of security events?	☒ Yes ☐ No
15.	Can the security credentials be upgraded remotely?	☒ Yes ☐ No ☐ No Credentials
16.	Can the security credentials be managed centrally?	☒ Yes ☐ No ☐ No Credentials
17.	Please list any security algorithms and standards used	See description of standards under J.
18.	Please provide additional information on how the standard addresses any “Yes” answers above	See description of standards under J.
19.	Please provide additional information about why any of the questions listed above do not apply to this standard	
	Logging and Auditing	
20.	Does the standard facilitate logging and auditing of critical operations and events?	☒ Yes ☐ No
21.	Can the standard gather statistics on its operation?	☒ Yes ☐ No ☐ Not applicable
22.	Can the standard report alerts and warnings?	☒ Yes ☐ No ☐ Not applicable
	Transaction State Management	
23.	Can the standard remotely enable or disable devices or functions?	☒ Yes ☐ No ☐ Not applicable
	System Preservation	
24.	Can the standard automatically recover from failed devices or links?	☒ Yes ☐ No ☐ Not applicable ☐ Provided in another layer
25.	Can the standard automatically re-route messages?	☐ Yes ☒ No ☐ Not applicable ☐ Provided in another layer
26.	Can the standard remotely determine the health (as opposed to just connectivity) of devices or software?	☒ Yes ☐ No ☐ Not applicable
	Other Management Capabilities	
27.	Please describe any other system or network management capabilities the standard provides.	IEC 62351-7 is the standard for network and system management
	Quality of Service	
28.	Is data transfer bi-directional?	☒ Yes ☐ No
29.	Can data be prioritized?	☒ Yes ☐ No ☐ Not applicable
30.	What types of reliability are provided?	☐ Reliable ☐ Non-guaranteed ☒ Both ☐ Either ☐ Provided in another layer
31.	Can information be broadcast to many locations with a single transmission?	☐ Yes ☐ No ☒ Not applicable
32.	Please describe any other methods the standard uses to manage quality of service.	
	Discovery and Configuration	
33.	Can the software or firmware be upgraded remotely?	☐ Yes ☐ No☒ Not applicable

Section II: Functional Description of the Standard		
34.	Can configuration or settings be upgraded remotely?	□ Yes □ No ☒ Not applicable
35.	Can implementations announce when they have joined the system?	□ Yes □ No ☒ Not applicable
36.	Can implementations electronically describe the data they provide?	□ Yes □ No ☒ Not applicable
	System Evolution and Scalability	
37.	What factors could limit the number of places the standard could be applied?	None per se
38.	What steps are required to increase the size of a system deploying this standard?	
39.	Is the information model separate from the transport method?	☒ Yes □ No
40.	Does the standard support alternate choices in the layers(s) below it?	☒ Yes □ No □ No layers below
41.	List the most common technology choices for layers implemented below this standard	Any, this is a security standard, not a protocol standard
42.	Does the standard support multiple technology choices in the layers above it?	☒ Yes □ No □ No layers above
43.	List the technologies or entities that would most commonly use this standard in the layer above	Any, this is a security standard, not a protocol standard
44.	Please describe any mechanism or plan to ensure the standard is as backward-compatible as possible with previous versions	
45.	Please describe how the design of this standard permits it to be used together with older or legacy technologies	Security can be turned off for equipment that cannot handle it
46.	Please describe how the design of this standard permits it to co-exist on the same network or in the same geographic area with similar technologies, and give examples	Protocols that use these security standards can co-exist on the same network with other protocols
47.	**Electromechanical**	

M. Architectural Principles

Please describe how this standard may apply any of these principles:

1.	Symmetry – facilitates bi-directional flow of energy and information	Not per se – but the protocols it secures can
2.	Transparency – supports a transparent and auditable chain of transactions	Part 7 is network and system management
3.	Composition – facilitates the building of complex interfaces from simpler ones	Not per se – but the protocols it secures can
4.	Loose coupling – can support bilateral and multilateral transactions without elaborate pre-arrangement	Not per se – but the protocols it secures can
5.	Shallow integration – does not require detailed mutual information to interact with other components	Not per se – but the protocols it secures can

Section II: Functional Description of the Standard

6.	Please list any other architectural models, reference architectures or frameworks this standard was designed to be compliant with, e.g. W3C, IEC TC57, OSI and how it fits those models	It is the security standard for IEC TC57.