

**Smart Grid Interoperability Panel (SGIP)
Cyber Security Working Group (CSWG)
Standards Review**

CSWG Standards Review Report

OASIS WS-Calendar

November 12, 2010

Security Assessment of PAP04: OASIS WS-Calendar

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different “layers” in the communications “stack” or “profile,” one example of such a profile is the GridWise Architecture Council (GWAC)¹ Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the “transport” layers for getting messages from one location to another. Still others cover the “application” layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into “bits and bytes” by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using “shall” statements, but rather use statements such as “should,” “may,” or “could.” Some standards also define their provisions as being “normative” or “informative.” Normative provisions often are expressed with “shall” statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the “shall,” “should,” “may,” and/or “could” statements, “normative,” or “informative” language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or “profile” of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both “power system” methods (e.g. redundant equipment,

¹GridWise Architecture Council, http://www.gridwiseac.org/pdfs/interopframework_v1.pdf

analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used. For some specific Smart Grid communication standards, such as International Electrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cybersecurity standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.3 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to “government-approved cryptography” refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees²:

- Requirements are expressed by “...shall...,” which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).

² The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after “which”) comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

- Recommendations are expressed by “...should...,” which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should equals is recommended that*).
- Permitted or allowed items are expressed by “...may...,” which is used to indicate a course of action permissible within the limits of the standard (*may equals is permitted to*).
- Ability to carry out an action is expressed by “...can ...,” which is used for statements of possibility and capability, whether material, physical, or causal (*can equals is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. “All traffic in this lane must turn right at the next intersection.”)

2. PAP04: OASIS WS-Calendar

The OASIS WS-Calendar standard is available at: http://www.oasis-open.org/committees/documents.php?wg_abbrev=ws-calendar.

2.1 Description of Document

The ws-calendar document states its scope as, “*WS-Calendar describes a limited set of message components and interactions providing a common basis for specifying schedules and intervals to coordinate activities between services. The specification includes service definitions consistent with the OASIS SOA Reference Model and XML vocabularies for the interoperable and standard exchange of:*

- *Schedules, including sequences of schedules*
- *Intervals, including sequences of intervals*

These message components describe schedules and intervals future, present, or past (historical). The definition of the services performed to meet a schedule or interval depends on the market context in which that service exists. It is not in scope for this TC to define those markets or services.”

The document provides an introduction to and a description of web services calendar, core and supplemental semantics, services and services characteristics.

2.2 Assumptions and Issues

This document covers the GWAC-stack “Semantic Understanding” and the “Syntactic Interoperability” layers. Therefore, all cybersecurity issues should be understood as applying only in those two contexts.

2.3 Summary of Cybersecurity Content

Security is not addressed in this document, and is explicitly excluded in the scope. For instance, section 7.1.3.1 of the document, identifies Access Controls as one of the issues not addressed by this specification. The document states that “*It is assumed that the targeted server will set an appropriate level of access based on authentication. This specification will not attempt to address the issues of sharing or Access Control Lists (ACLs).*” (Section 7.1.3.1 Access Control, page 44 of 76).

2.3.1 Does the standard address cybersecurity? If not, should it?

The standard does not address security, but either it or a corresponding document should address security. It is important that security requirements be included in Services design standards. If these schedules become the basis for scheduling and private publishing for energy transactions across multiple independent system operator (ISO) and regional transmission organization (RTO) domains, then transactions involving authentication and non-repudiation should be included in the design.

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

The standard does not address security within it. It is not certain as to whether future releases will address security either by inclusion or reference.

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard ³	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
<i>None</i>		

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

The CSWG recommends that this document be accepted as is, but that corresponding documents be developed in future efforts (in a DEWG or PAP) that:

- Provide security requirements at the Syntactic Interoperability layer for ws-calendar transactions. These security requirements should cover confidentiality, integrity and availability, either by inclusion, reference, or both.
- Provide security guidance for those information model standards that consist substantially of XML-based data structures. Such guidance can reference existing standards and explain alternatives and options for applying them to secure files and communications exchanges in XML-based formats

2.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

Next steps for the OASIS Technical Committee on ws-calendar are not known.

2.3.5 List any references to other standards and whether they are normative or informative.

Normative and Non normative References are included below:

³ The references may be just the section numbers or could include the title of the section

2.3.5.1 Normative References

- Calendar Resource Schema** C. Joy, C. Daboo, M Douglas, *Schema for representing resources for calendaring and scheduling services*, <http://tools.ietf.org/html/draft-cal-resource-schema-00>, (Internet-Draft), April 2010.
- FreeBusy Read URL** E York. *Freebusy read URL*, <http://www.calconnect.org/pubdocs/CD0903%20Freebusy%20Read%20URL%20V1.0.pdf>
- RFC2119** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, <http://www.ietf.org/RFC/RFC2119.txt>, IETF RFC2119, March 1997.
- RFC2447** F. Dawson, S. Mansour, S. Silverberg, *iCalendar Message-Based Interoperability Protocol (iMIP)*, <http://www.ietf.org/RFC/RFC2247.txt>, IETF RFC2447, December 2009.
- RFC2616** R Fielding, et al. et al, *Hypertext Transfer Protocol -- HTTP/1.1* <http://tools.ietf.org/html/RFC2616>, IETF RFC2616, November 1998
- RFC3339** G Klyne, C Newman, *Date and Time on the Internet: Timestamps* <http://tools.ietf.org/html/rfc3339>
- RFC4791** Daboo, et al. *Calendaring Extensions to WebDAV (CalDAV)*. <http://www.ietf.org/rfc/rfc4791.txt>. IETF RFC 2119, March 2007
- RFC4918** L. Dusseault, *HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)* <http://tools.ietf.org/html/rfc4918>
- RFC5545** B. Desruisseaux *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*, <http://www.ietf.org/rfc/rfc5545.txt>, IETF RFC5545, September 2009.
- RFC5546** C. Daboo *iCalendar Transport-Independent Interoperability Protocol (iTIP)*, <http://www.ietf.org/rfc/rfc5546.txt>, IETF RFC5546, December 2009.
- SOA-RM** OASIS Standard, *Reference Model for Service Oriented Architecture 1.0*, October 2006. <http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf>
- Web-Linking** M. Nottingham, *Web linking*. <http://tools.ietf.org/html/draft-nottingham-http-link-header> May 2010
- draft xCal** C. Daboo, M Douglas, S Lees *xCal: The XML format for iCalendar*, <http://tools.ietf.org/html/draft-daboo-et-al-icalendar-in-xml-03>, Internet-Draft, April 2010.
- XPATH** A Berglund, S Boag, D Chamberlin, MF Fernández, M Kay, J Robie, J Siméon *XML Path Language (XPath) 2.0*, <http://www.w3.org/TR/xpath20/> January 2007.
- XLINK** S DeRose, E Maler, D Orchard, N Walsh *XML Linking Language (XLink) Version 1.1.*, <http://www.w3.org/TR/xlink11/> May 2010.
- XPOINTER** S DeRose, E Maler, R Daniel Jr. *XPointer xpointer Scheme*, <http://www.w3.org/TR/xptr-xpointer/> December 2002.
- XML SCHEMA** PV Biron, A Malhotra, *XML Schema Part 2: Datatypes Second Edition*, <http://www.w3.org/TR/xmlschema-2/> October 2004.
- XRD** OASIS XRI Committee Draft 01, *Extensible Resource Descriptor (XRD) Version 1.0*, <http://docs.oasis-open.org/xri/xrd/v1.0/cd01/xrd-1.0-cd01.pdf> October 2009.

2.3.5.2 Informative References

- NIST Framework and Roadmap for Smart Grid Interoperability Standards**, Office of the National Coordinator for Smart Grid Interoperability, Release 1.0, NIST Special Publication 1108,
http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.
- NAESB Smart Grid Requirements** (*awaiting publication*) (*draft contributed*)
<http://lists.oasis-open.org/archives/ws-calendar-comment/201005/doc00000.doc>,
May 2010
- REST** T Fielding, *Architectural Styles and the Design of Network-based Software Architectures*, <http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm>.
- TZDB** P Eggert, A.D. Olson, "Sources for Time Zone and Daylight Saving Time Data", <http://www.twinsun.com/tz/tz-link.htm>
- Time Zone Recommendations**, CalConnect, *CalConnect EDST (Extended Daylight Savings Time) Reflections and Recommendations*, Version: 1.1,
<http://www.calconnect.org/pubdocs/CD0707%20CalConnect%20EDST%20Reflections%20and%20Recommendations%20V1.1.pdf>
October 2010
- Time Zone Service**, M Douglas, C Daboo, *Timezone Service Protocol*, Draft RFC,IETF,
<http://datatracker.ietf.org/doc/draft-douglass-timezone-service/>
2007-07-05