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

CSWG Standards Review Report

Zigbee Smart Energy Profile 2.0 Technical Requirements Document (TRD), 095449 Version 0.7

May 10, 2011

Security Assessment of Zigbee Smart Energy Profile 2.0 Technical Requirements Document (TRD), 095449 Version 0.7

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) 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, 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.

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

1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may, in fact, be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

1.3 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.

1.4 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 degrees[1]:

- 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*).
- 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. Zigbee Smart Energy Profile 2.0 Technical Requirements Document (TRD), 095449 Version 0.7

2.1 Description of Document

The Draft Smart Energy Profile (SEP) 2.0, version 0.7, consists of two related documents:

1. Zigbee Smart Energy Profile 2.0 Technical Requirements Document
2. Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification

According to the Zigbee Smart Energy Profile 2.0 Technical Requirements Document (TRD), the purpose of this document (SEP 2.0, ver.7, TRD) is "*to provide a clear set of technical requirements for implementing Zigbee Smart Energy Profile 2.0 on Zigbee, HomePlug, Wi-Fi, Ethernet, and other IP-capable platforms. These technical documents are based on marketing requirements provided in the Zigbee + HomePlug Smart Energy 2.0 MRD [ZBHP MRD], or inferred by the technical team. To the extent that the Zigbee and HomePlug networking technologies are specifically mentioned in the MRD, appropriate requirements for their support of Zigbee Smart Energy Profile 2.0 are defined in this document. Throughout this document, other MAC/PHYs may be mentioned by name as illustrative examples or partial lists. These references are not intended to convey any preference for the named MAC/PHY(s) over any other MAC/PHY(s) that may support Zigbee Smart Energy Profile 2.0.*"

The TRD also states that:

[1] 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.

"*… the requirements in this document are organized by layers. These layers correspond roughly with the Internet Protocol Stack layers, with the addition of an adaptation layer, necessary to bridge between conventional IPv6 and selected substrates.*"

The adaption layer is constrained further by the Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification, namely:

"*This draft document is also intended to enable communications that are link layer agnostic and run over the Internet Protocol (particularly IPv6).*"[2]

2.2 Assumptions

General assumptions on security in section 1.6.3 state, "*Assume Devices WILL be physically compromised and make certain this does not lead to further compromises over the network.*"

The TRD is limited to requirements for "*a networking and application integration platform for messages between customer Devices and Energy Service Providers.*" It is not clear whether this implies communications outside the Home Area Network (HAN) or just from the Energy Services Interface (ESI) into the HAN.

Section 12 of the Draft SEP 2.0 TRD covers cybersecurity requirements. It states: "*In designing the overall security of a system we consider the fundamental security services typically provided by cryptography, and take as a general principal that selecting the right technology based on designing for a scarcity of resources prevalent in embedded systems and selecting mechanisms that provide multiple security services.*" This leaves the security requirements for end-to-end security unaddressed.

Section 13 of the Draft SEP 2.0 TRD indicates that the specification "*covers HAN Devices which can be managed by the Service Provider. Examples of devices not covered include: home automation, home health monitoring, and security system products...*", therefore restricting the use of Zigbee devices to HAN, requiring that on a network there will be at least two devices and the "*Devices shall be an Energy Services Interface (ESI) or a Device capable of Authorizing network join and admission*" and "*Each instance of the HAN may support more than one Edge Router.*"

There is a requirement stating "*SE 1.0 devices MUST be able to communicate with SE 2.0 Devices*" and this requirement is met by "*Upgrading existing devices supporting upgrading; [or] Replacing existing devices with new Devices [or] Using a proxy/gateway between the Smart Energy Profile Network and existing devices.*".

2.3 Assessment of Cybersecurity Content

The TRD section 12 lays out the security required tenets of the requirements. These include:

1) Confidentiality – being "*the property whereby information is not disclosed to unauthorized parties;*"
2) Data Integrity – being "*a property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored;*"
3) Authentication – being "*a service that is used to establish the origin of information;*"
4) Authorization – being "concerned with providing an official sanction or permission to perform a security function or activity;" and
5) Non-repudiation – being "*a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party.*"

[2] Note that the acronym "SEP" and "SE" appear to be used interchangeably.

The document continues to identify additional non cryptographic tenets of security such as: physical security, identity, availability, audit, and administration. However these are not fully defined in this TRD.

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

Section 12 addresses cybersecurity.

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

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
12.3 Cryptographic strength	SG.SC-12: Use of Validated Cryptography	The requirements only cover the strength of the cryptography, not specific algorithms. It does not mention NIST validated cryptography.
12.4 Key Establishment	SG.SC-11: Cryptographic Key Establishment and Management	Touches on key management establishment, but does not specify any specific process or requirements.
12.6.2 Layer 2 – Link Layer	SG.SC-14: Transmission of Security Parameters	
12.6.3 Layer 3 – Network Layer	SG.SC-11: Cryptographic Key Establishment and Management	Assumes IPv6 will be used, which is not a valid assumption. Includes DES, MD5, and other cryptographic suites which are no longer considered acceptable.
12.6.4 Layer 4 – Transport Layer	SG.SC-11: Cryptographic Key Establishment and Management	Describes TLS and UDP, stating that many different cryptographic suites are available. However, it does not deprecate any in accordance to NIST validated cryptography requirements. Specifically, DES, 3DES, SHA-1, and MD5 should be deprecated.
12.7.3 (Security) Procedures	SG.IA-5: Device Identification and Authentication	This section includes simple tutorial statements without actual security requirements.
12.8 Network Environment Security	SG.IA-5: Device Identification and Authentication	General requirement that an Authenticated Key Agreement scheme should be used to gain access to the Network. Different alternatives are also discussed.
12.8.1 Authentication Option 1: (End-Device	SG.IA-5: Device Identification and Authentication	It is unclear what is meant by an unpredictable Authentication code.

[3] The references may be just the section numbers or could include the title of the section, depending upon what fits easily.

PIN/Passphrase)		
12.9 Application Environment Security	SG.IA-5: Device Identification and Authentication	The processes for device authentication and authorization are not explicitly defined – just that they are needed. For instance, there is no discussion of role-based access control.
12.10 Identification	SG.IA-5: Device Identification and Authentication	
12.13 Auditing	SG.AU-2: Auditable Events	Only Devices that require Non-Repudiation must have audit logs. However, there are many other reasons, such as cybersecurity events, sequence-of-events of power events, that are critical for maintaining audit logs.
12.15.2 Cryptographic Protocols	SG.SC-12: Use of Validated Cryptography	These cryptographic protocols come from the Market Requirements Document. The list should be checked against the NIST list of approved cipher suites.
12.17.2 Cryptographic cipher suites based on Transport Layer Security (TLS)	SG.SC-12: Use of Validated Cryptography	This section discusses specific cipher suites, and includes the statement, "*Only security functions which are referred to directly or indirectly by FIPS 140-2 as Approved security functions will be considered*."
12.18 Security Policies	SG.SC-12: Use of Validated Cryptography	The focus of this section on security policy is still on cryptography. It does not address the larger security policy issues.

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?

- **Lack of clarity due to mixture of tutorial and requirements** – The SEP 2.0 TRD is a mixture of tutorial/informative material and specific normative requirements which is an effective method for ensuring understanding of an issue while also defining the exact requirements. However, the normative requirements do not always cover the same issues as the informative material, or only partially address the issues raised. Therefore, this approach leaves open many questions on whether some of the informative material should also be understood as acceptable. For instance, DES is mentioned in the tutorial material, but it is not deprecatedper NIST FIPS 140-2, nor otherwise indicated that it should not be used.
- **Focus on encryption rather than end to end security** – The document initially implies that encryption is the only necessary security requirement, rather than policies, procedures, and many other types of security technologies. Although some of these aspects may be outside the scope of this document, references to existing and planned documents on these aspects of SEP 2.0 should be provided.
- **Lack of certificate and key management requirements** – Key and certificate management must be addressed to ensure that a proper method of revocation and renewal are included. Many solutions currently do not provide a means of revoking and renewing keys and/or certificates. Many also do not provide for a certification revocation list (CRL), therefore, if a revocation process is available, there is no means of verifying whether a certificate has been revoked.
- **Lack of addressing vulnerability management** – It is vital to have the ability to distribute vulnerability remediations to devices in the field to ameliorate the inevitable attempts to gain

control of the devices. Encryption alone does not solve many vulnerability issues; there is a need for end-to-end security.

- **Lack of malware management requirements** – As devices become more prominent in the market, there is the potential for new malware to infect these devices. Methods for protecting devices against unauthorized programs and processes on a SEP network must be addressed.
- **Lack of intrusion detection and prevention requirements** – SEP systems must include the ability to detect and prevent intrusions. One method could include requiring vendors to "describe" what their clean devices look like so that anomaly detection processes can be written for these devices.
- **Lack of tamper protection and identification requirements** – Tamper protection and identification, especially for items such as Home Energy Managers (HEM), Load Control Switches (LCS) and other devices that may reside on the outside of the premise, will be necessary. This will include the requirement to log events of tamper or tamper attempts.
- **Lack of forensic logging requirements** – Standard or minimum requirements for audit logs, including the minimum accuracy of time stamps, should be specified to ensure being able to trace across different devices and different networks.
- **Requirement that only IPv6 is used.** SEP 2.0 should not prevent the use of IPv4. The IPv6 security issues must be addressed including the fact that IPv6 exposes the IP address of the private end device to the larger network.
- **Section 10 mixes the general services provided by the Application Layer with very specific functional requirements** – SEP 2.0 should separate the messaging service requirements described in Section 10.3 from the very specific functional requirements of different applications described in the remaining subsections of Section 10 – the latter should be removed from this document and placed in a separate modeling document. This is a serious security issue in that it is inevitable that the specific requirements will have to be changed, but the general requirements should continue to be valid. The moment one major change is made and the SEP document is no longer definitive, the security of the entire system becomes vulnerable to other changes.
- **Section 10 describes functions, but does not address their security**. For example:
  - **Section 10.7** – the security of the accounting information in the meter is not addressed.
  - **Section 10.8** – the security of the additional meters for DER is not addressed
  - **Section 10.10** – the security for PEVs during roaming is not addressed
- **Certain cryptographic suites should be deprecated** in Sections 12.6.3 and 12.6.4, including DES, 3DES, SHA-1, and MD5.

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

The draft SEP 2.0 documents are being reviewed and commented on by many stakeholders, including the CSWG. As an output of the public comment and this review, it is anticipated that many of the existing security issues will be addressed in future versions.

2.3.5 Recommendations

This document does not meet the requirements of the NISTIR at this time. The CSWG recommends that the SGIP not accept this SEP 2.0 document until the following recommendations are acted upon:

- Remediate the security issues identified in section 2.3.3, either by direct inclusion in the document or as normative references to existing document or by planning future documents to address the security issues.
- Specifically, the Security Tenets in section 12.1 of the TRD document should acknowledge broader cybersecurity approaches than just those provided by cryptography.
- The assumption that IPv6 will be used universally is not valid. Security for IPv4 should also be included, including for gateways between IPv4 and IPv6.
- Cipher suites that are no longer approved by NIST FIPS 140-2 are included in Section 12.6. At a minimum, these should be indicated as no longer approved. It would be preferable to remove these cipher suites from the document as the recommended set of cipher suites are described in 12.17.2
- The specific functional requirements should be removed from Section 10.x to avoid the inevitable non-compliance with those detailed sections from impacting compliance with the more general Application Layer requirements. The mix of functional requirements and general Application Layer requirements poses a security risk that other non-compliance decisions will be more easily undertaken, including non-compliance with the security requirements in Section 12, etc.
- Recommend at least 3072 bits for RSA crypto suites.
- Recommend the identification of the following crypto suites for TLS from NIST SP800-53, table 3 as the minimum preferred suites:
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DH_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_DH_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CCM_8
- Recommend the identification of the ECC crypto suites from RFC5430 as the minimum preferred suites:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

Clarify which references are normative and which are informative.

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

2.3.6.1 Normative and/or Informative References (not distinguished)

Zigbee+HomePlug Liaison Documents

ZBHP MRD	• ZigBee+HomePlug Joint Working Group Smart Energy Profile Market

	Requirements Document (http://www.zigbee.org/imwp/download.asp?ContentID=16081)

Zigbee Alliance Documents

ZB 053474	• ZigBee Specification (053474r17)
ZB 075123	ZigBee Cluster Library Specification (ZCL) (075123r02)
ZB 075356	Smart Energy Profile (075356r15)
ZB 094940	SEP Intermediate Release 1 MRD (094940)
ZB 095021	SEP Intermediate Release 1 TRD (095021)
ZB 095310	SEP Intermediate Release 1 Profile Specification (095310)
ZB 095165	Prepay requirements for the Intermediate release (095165)
ZB 095208	SE PM Additional Incremental Release Features (095208)
ZB 095288	Smart_Water_Meter_MRD (095288r00)
ZB 095328	Smart Energy Profile UML Model (095328)

IEC Documents

All IEC documents are available at: http://webstore.iec.ch, unless otherwise specified.

61850	Communication networks and systems in substations - ALL PARTS
61850-1	Communication networks and systems in substations - Part 1: Introduction and overview
61850-7-420	Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes
61968-1	Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general requirements
61968-2	Application integration at electric utilities - System interfaces for distribution management - Part 2: Glossary
61968-3	Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations
61968-4	Application integration at electric utilities - System interfaces for distribution management - Part 4: Interfaces for records and asset management
61968-9	Application integration at electric utilities - System interfaces for distribution management - Part 9: Interfaces for meter reading and control
61968-13	Application integration at electric utilities - System interfaces for distribution management - Part 13: CIM RDF Model exchange format for distribution
61968 UML	CIM Users Group Unified Modeling Language (UML) Model http://cimug.ucaiug.org/CIM%20Model%20Releases/Forms/AllItems.aspx)
61970-301	Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM) base
62055-21	Electricity Payment Meters – A Framework for Standardization

IEEE Documents

802.15.4	IEEE 802.15.4-2006, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) (http://standards.ieee.org/getieee802/)
802.1AR	IEEE P802.1AR/D2.2: Draft Standard for Local and Metropolitan Area Networks: Secure Device Identity (http://employees.org/%7Eczmax/802.1AR/802-1ar-d2-2.pdf)
802.1X	IEEE 802.1X: IEEE Standard for Local and Metropolitan Area Networks: Port Based Access Control (http://standards.ieee.org/getieee802/)
IEEE 1363a	IEEE, 1363a -2004, IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques (The IEEE Shop)
IEEE P1901	IEEE 1901(tm)-2010, IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications (The IEEE Shop)

IETF Documents

RFC 768	User Datagram Protocol (http://tools.ietf.org/html/rfc768)
RFC 792	Internet Control Message Protocol (http://tools.ietf.org/html/rfc792)
RFC 793	Transmission Control Protocol (http://tools.ietf.org/html/rfc793)
RFC 1042	A Standard for the Transmission of IP Datagrams over IEEE 802 Networks (http://tools.ietf.org/html/rfc1042)
RFC 1208	A Glossary of Networking Terms (http://tools.ietf.org/html/rfc1208)
RFC 2080	RIPng for IPv6 (http://tools.ietf.org/html/rfc2080)
RFC 2409	The Internet Key Exchange (IKE) (http://tools.ietf.org/html/rfc2409)
RFC 2119	Key words for use in RFCs to Indicate 401 Requirement Levels (http://tools.ietf.org/html/rfc2119)
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification (http://tools.ietf.org/html/rfc2460)
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (http://tools.ietf.org/html/rfc2545)
RFC 2616	Hypertext Transfer Protocol -- HTTP/1.1 (http://tools.ietf.org/html/rfc2616)
RFC 2631	Diffie Hellman Key Agreement Method (http://tools.ietf.org/html/rfc2631)
RFC 3117	IETF RFC 3117, On the Design of Application Protocols (http://tools.ietf.org/html/rfc3117)
RFC 3748	Extensible Authentication Protocol (EAP) (http://tools.ietf.org/html/rfc3748)
RFC 3766	IETF RFC 3766, Determining Strengths For Public Keys Used For Exchanging Symmetric Keys (http://tools.ietf.org/html/rfc3766)
RFC 4279	Pre-Shared Key Ciphersuites for Transport Layer Security (http://tools.ietf.org/html/rfc4279)
RFC 4291	IP Version 6 Addressing Architecture (http://tools.ietf.org/html/rfc4291)[RFC 4302] IP Authentication Header (http://tools.ietf.org/html/rfc4302)
RFC 4303	IP Encapsulating Security Payload (ESP) (http://tools.ietf.org/html/rfc4303)
RFC 4306	Internet Key Exchange (IKEv2) Protocol (http://tools.ietf.org/html/rfc4306)

RFC 4347	Datagram Transport Layer Security (http://tools.ietf.org/html/rfc4347)
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (http://tools.ietf.org/html/rfc4443)
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (http://tools.ietf.org/html/rfc4492)
RFC 4861	Neighbor Discovery for IP Version 6 (IPV) (http://tools.ietf.org/html/rfc4861)
RFC 4862	IPv6 Stateless Address Autoconfiguration (http://tools.ietf.org/html/rfc4862)
RFC 4919	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals (http://tools.ietf.org/html/rfc4919)
RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks (http://tools.ietf.org/html/rfc4944)
RFC 5191	Protocol for Carrying Authentication for Network Access (PANA) Framework (http:/tools.ietf.org/html/rfc5191)
RFC 5216	The EAP-TLS Authentication Protocol (http://tools.ietf.org/html/rfc5216)
RFC 5238	Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP) (http://tools.ietf.org/html/rfc5238)
RFC 5246	The Transport Layer Security (TLS) Protocol v1.2 (http://tools.ietf.org/html/rfc5246)
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework (http://tools.ietf.org/html/rfc5247)
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS (http://tools.ietf.org/html/rfc5288)
RFC 5289	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) (http://tools.ietf.org/html/rfc5289)
RFC 5340	OSPF for IPv6 (http://tools.ietf.org/html/rfc5340)
ID-6ND	6LoWPAN Neighbor Discovery, IETF Internet Draft, (http://tools.ietf.org/html/draft-ietf-6lowpan-nd-11)

Other References

EXI	Efficient XML Interchange (EXI) Format 1.0 (http://www.w3.org/TR/2008/WD-exi-20080919/)
REST	Representational State Transfer (http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm)
XEP-0134	Protocol Design Guidelines (http://xmpp.org/extensions/xep-0134.html)

Security References

ANS X9.31	ANS X9.31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
ANS X9.44	ANS X9.44, Public-Key Cryptography for the Financial Services Industry Key Establishment Using Integer Factorization Cryptography (http://www.nssn.org/)
ANS X9.62	ANS X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic

	Curve Digital Signature Algorithm (ECDSA) (http://www.nssn.org/)
ANS X9.63	ANS X9.63, Public Key Cryptography for the Financial Services Industry Key Agreement and Key Transport Using Elliptic Curve Cryptography.(http://www.nssn.org/)
FIPS 140-2	NIST FIPS 140-2, Security Requirements for Cryptographic Modules (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
FIPS 180-3	NIST FIPS 180-3, Secure Hash Standard (http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf)
FIPS 197	NIST FIPS 197, Advanced Encryption Standards (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)
FIPS 198-1	NIST FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC) (http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf)
SEC1	SECG SEC1, Standards for Efficient Cryptography Group, SEC 1, (http://www.secg.org/download/aid-780/sec1-v2.pdf)
SEC4	SECG SEC 4, Elliptic Curve Qu-Vanstone Implicit Certificate 471 Scheme (ECQV) Compatible Description: Proposed new work item for ANS X9 F1. (http://www.secg.org/download/aid-775/sec4-ECQV-v091.pdf)
SP 800-38C	NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality (http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf)
SP 800-57-1	NIST SP 800-57, Recommendation for Key Management (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1- revised2_Mar08-2007.pdf)
SP800-56A	NIST SP800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf)
SP800-56B	NIST SP800-56B, Recommendation for Pair-Wise Key Establishment Schemes: Using Integer Factorization Cryptography (http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf)
X.509	ITU X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (http://www.itu.int/rec/T-REC489 X.509/en)
X.690	ITU X.690 : Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (http://www.itu.int/rec/T-REC-X.690/en)

UCA References

OpenHAN	UCAIug Home Area Network System Requirements Specification (http://osgug.ucaiug.org/sgsystems/openhan/Shared%20Documents/OpenHAN %202.0/UCAIug%20HAN%20SRS%20-%20v2.0.pdf)

SAE References

SAE J2836/1™	SAE J2836/1™ Use Cases for Communication between Plug-in Vehicles and the Utility Grid (Surface Vehicle Information Report)
SAE J2836/2™	SAE J2836/2™ Use Cases for Communication between Plug-in Vehicles and the Supply Equipment (EVSE) (Surface Vehicle Information Report)
SAE J2836/3™	SAE J2836/3™ Use Cases for Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow (Surface Vehicle Information Report)
SAE J2836/5™	SAE J2836/5™ Use Cases for Communication between Plug-in Vehicles and their customers (Surface Vehicle Information Report)
SAE J2847/1	SAE J2847/1 Communication between Plug-in Vehicles and the Utility Grid (Surface Vehicle Recommended Practice)
SAE J2847/2	SAE J2847/2 Communication between Plug-in Vehicles and the 508 Supply Equipment (EVSE) (Surface Vehicle Recommended Practice)
SAE J2847/3	SAE J2847/3 Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow (Surface Vehicle Recommended Practice)