

## Cyber Security (CSWG) Assessment of PAP-11

Status: Not Approved

Were CSWG requirements met? No

Comments: The CSWG is recommending that PAP-11 not be approved due to cybersecurity issues identified within SAE J2847-1, *Communication between Plug-in Vehicles and the Utility Grid*. The following families of National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, high-level security requirements are not addressed and should be addressed at some level in this or a referenced document:

- Access control (SG.AC) (e.g. passwords, least privilege, role-based access control);
- Auditing and accountability (SG.AU);
- Security assessment (SG.CA);
- Continuity of operations (SG.CP) is addressed functionally (e.g. on loss of communications) but not for security (e.g. security breach);
- Identification and Authentication (SG.IA) is addressed in that devices have IDs, but is not addressed with respect to security (authentication);
- Incident Response (SG.IR) is not addressed even from a functional level;
- Media Protection (SG.MP) is not addressed except functionally that PLC is more likely to be secure than wireless media;
- Information System and Services Acquisition (SG.SA) is not addressed, including supply chain protection; and
- System and Communication Protection (SG.SC) is not addressed above the Network Layer, nor is key management at the Network Layer.

Additionally, the following more specific issues are also noted:

- If PLC, wireless, or other potentially radiating technology is used for the communications, the traffic between the PEV and the EVSE should be encrypted. If no encryption, shielding, or other electromagnetic protection methods are used, there is a potential that confidential information (e.g., vehicle ID, credit card numbers, etc.) may be radiated in the clear between the EVSE and the PEV over power line carrier or wireless media.
- Section 4.3.3.2 refers to a customer PIN being entered through a "NAV" which is otherwise undefined. If the NAV is inside the car, encryption may be required for exchange with the EVSE.
- There are some decisions that need to be made regarding the use of TLS that are unaddressed. For example, what to do if a certificate expires.
- There may be some further information that needs to be specified about the use of EXI. Some of that information involves defining the MIME types if EXI is used with XML Encryption so the decoder will properly interpret the message.
- Since this is Recommended Practice, the word "shall" should not be used for any items that are just being recommended, not mandated.
- Any security Use Cases that will be added should be reflected in this document (or if security is deleted from this document, as recommended, addressed in the appropriate security document).
- There is absolutely no mention of a privacy policy governing anything in this standard. There is no mention of giving customer notice of information being collected and stored. Neither is there any consent requested or

choice given as to what is being collected. The data to be collected is defined, but what that data is being used for is fairly open-ended.

- Within the messages being exchanged from the EUMD or PEV to the utility are data items that specifically identify the PEV (VIN) and the individual customer (Account Number, other?). Also exchanged may be information on charging location as well as some undefined, for the most part, user preferences. General privacy issues result from a lack of definition on what data is being collected and stored, lack of specifics on how customer specific data will be limited/protected, and a number of instances in which it says the utility may want to collect data for statistical or other purposes.
- In Section 4.3.3 – The subsection on Identification Messaging outlays the collection of data that will uniquely identify a PEV and/or a customer. One suggestion for the customer ID is the account number the utility has on file for the customer. There are no other suggestions given, or limitations on what should not be used (SSN, for instance). A suggestion for the vehicle ID is the VIN. Some may have privacy concerns over the use of a VIN.
- In Section 4.3.6 – The Subsection on Timing Information messaging notes that charging information specific to each customer may be collected and used for other purposes. To the extent that there are privacy implications with the possible release of this data, this standard does not limit, or otherwise define how the data being gathered can be used.
- In Section 4.3.6.3 – It is left to the equipment manufacturer to determine what historical data is retained to assist customers in explaining potential deviations in pricing. While there may not be a privacy concern with the storage of requests for pricing data, data retention risks and recommendations should be referenced. It is not clear why the utility or the customer should not be in charge of the settings that control collection of historical data, as opposed to the OEM.
- In Section 4.3.7.2 – This notes that, while it is not necessary to collect and gather SOC information, the utility may want to do it for other purposes, specifically compiling usage statistics or grid management purposes. One of the principles recommended by the SGIP-CSWG Privacy Subgroup is to collect only the information necessary to provision service. If this information is not necessary for such purpose, should it be collected? If so, should there be some notice to the customer that such information is being collected for purposes other than providing service to that customer. Further, if data is going to be gathered, that means retention and perhaps there should be some discussion of retention standards, or that utilities should follow applicable retention standards (not that the U.S. has any).
- The underlying architectural assumptions may have cybersecurity concerns, such as privacy violations and/or identity theft possibilities if EVSEs are compromised.

In general, SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid does not include security for the GWAC-stack Syntactic Interoperability layer nor the Semantic Understanding layer, even though information exchange requirements at those layers are described in the SAE document. The discussions of security at the Network Interoperability layer are inadequate and inappropriate for the focus of this document.

Given these serious deficiencies in addressing cybersecurity, the CSWG recommends the following:

- Remove all references to cybersecurity and develop a separate, corresponding cybersecurity document. Because there are many missing cybersecurity requirements, it is recommended that Section 4.3.1.2 and all references to cybersecurity be removed from this document and that another document or documents be developed to address cybersecurity for these information exchanges.
- Remove the mapping to SEP2.0 in order to separate semantic standards from their mappings to different protocols that will have different cybersecurity technologies. Because the SEP 2.0 protocol is not yet defined,

may not be used by utility operational systems, and because other protocols could be used to support the messages defined in Section 4.3 in different architectures with different cybersecurity technologies, it is recommended that Section 4.4 be removed in order to keep the semantic standards separate from the various protocols which could transport those messages.

- Ensure consistency with the results of other PAPs. Role of the Internet Protocol Suite (IPS) in the Smart Grid, developed as an output of PAP 01,<sup>1</sup> does not include EAP (RFC 3748), but instead identifies EAP-TLS (RFC 5216), which in turn references EAP (RFC 3748). Consistency between PAP 1 and PAP 11 would be a good goal, but is not absolutely required.
- Reference the FIPS-approved list of cryptography suites. The acceptable cyber cryptography suites are listed, which may limit future applicability. It is suggested that the document reference the Federal Information Processing Standard (FIPS)-approved list of cryptography suites.
- References to unfinalized IETF RFCs should be removed. The reference to IETF RFC 4492 should be removed until the IETF finalizes the RFC.

However, SAE J2836/1, *Use Cases for Communication Between Plug-in Vehicles and the Utility Grid*, and SAE J1772-TM, *SAE Electric Vehicle Plug-In Hybrid Electric Vehicle Conductive Charge Coupler*, had no critical gaps in cybersecurity to prevent sign-off and approval. The CSWG suggests the following considerations for the next revision cycle and review of the standard:

- **SAE J2836/1**
  - a) It is recommended that this standard be accepted as is, but that additional cybersecurity Use Cases be developed during the next V2G PAP and/or DEWG efforts.
  - b) The normative and informative reference document list within SAE J2836/1 should also be reviewed to determine if any cybersecurity requirements in those documents need to be updated or enhanced.
- **SAE J1772-TM**
  - a) If PLC, wireless, or other potentially radiating technology is used for the communications, the traffic between the PEV and the EVSE should be encrypted. If no encryption, shielding, or other electromagnetic protection methods are used, there is a potential that confidential information (e.g., vehicle ID, credit card numbers, etc.) may be radiated in the clear between the EVSE and the PEV over power line carrier or wireless media.
  - b) The normative and informative reference document list within SAE J1772-TM should be reviewed to determine if any cybersecurity requirements in those documents need to be updated or enhanced.

The CSWG strongly recommends that SAE J2847-1, *Communication between Plug-in Vehicles and the Utility Grid*, be removed from the results of PAP 11 and taken up by the next V2G PAP and/or DEWG for completion in order to ensure that cybersecurity is adequately addressed. Once the document is removed from the PAP 11 results, the CSWG will approve the remaining PAP 11 results.

---

<sup>1</sup> SGIP PAP 1: *Internet Protocols for the Smart Grid*: draft-baker-ietf-core-09