# SG Security (UtiliSec) Face-to-Face

**Meeting Minutes**

**October 21, 2009**

**Chair** – Darren Highfill/ SCE, Saker Systems
**Co-Chair** – Matt Carpenter/ Consumers, InGuardians
**Secretary** – Bobby Brown/ Consumers, EnerNex

**Attendees**:

Brad Johnson/ Oncor
Brian Smith/ EnerNex
Charles Spirakis/ Google
Chuck Duffy/ Cisco
Daniel Thanos/ GE
Doug Houseman/ EnerNex
Ed May/ Itron
Eric Johnson/ Eon US
Frances Cleveland/ Xanthus
Galen Rasche/ Southwest Research Inst.
Gary Birk/ Aclara
Gary Finco/ Idaho National Lab
Gillis Melancon/ FPL
Isaac Ghansah/ CA State University of Sacramento
James Ivers/ SEI
James Nutaro/ ORNL
James Stoupis/ ABB
Jeff McCullough/ Elster
Joe LoPorto/ PHI
John Lilley/ SDG&E
John Marinuzzi/ Boeing
Kay Clinard/ UCAIug
Ken Jones/ Elster
Kevin Fennell/ Landis+Gyr
Kip Gering/ Itron
Kris Brown/ Price Waterhouse Coopers
Kurt Stammberger/ Mocana
Lindani Phiri/ Elster
Lizardo Hernandez/ Landis+Gyr
Nick Gerbino/ Dominion
Oliver Johnson/ Tendril
Paul Duffy/ Cisco
Robert Jepson/ Lockheed Martin
Sandy Bacik/ Sensus
Shawn Hu/ Extensible Solutions
Stephen Chasko/ Landis+Gyr
Terry Dillon/ APS
Tom Overman/ Boeing
Vincent Bemmel/ Trilliant
Viola Lee/ PG&E
Wayne Longcore/ CMS Energy
William Godwin/ Progress Energy
Xiaoming Feng/ ABB

# 1.0 Joint Session OpenADE & SG Security

Dave Mollersuen (Tendril), Chair OpenADE / Steve Van Ausdil (Xtensible Solutions), Darren Highfill (Chair SG Security)

## *1.1 Overview*

Charter – is available on Smartgidipedia.org, includes scope. Consumer utility data initial scope includes getting data from the utility directly. Want to get to market directly. There is a broader vision for what want to do down the road. Want to get to a 1.0 requirements spec and will do an SRS next. The security team will begin getting involved at SRS-level.

Schedule is on smartgridipedia.org. Third parties that will have access include Google, Tendril, and so on. A consumer grants access to consumption data and have utilities to routinely pull and aggregate and display for third parties.

User requirements has section on what may be looking at in the future.

“Automated” refers to the automatic data exchange after the relationships have been setup on the respective systems.

## *1.2 Status*

Currently at v-0.98 of the business and user requirements document; currently under ballot. The overall timeline is that real close to finishing of the user requirements – would be equivalent to a marketing document. And solid SRS to be ready for ballot by next face-to-face in January 2010.

## *1.3 ASAP-SG / SG Security (Darren)*

ASAP-SG funded project to get work done for UtiliSec. ASAP-SG is doing security profiles. First is AMI. The second is Third Party Data Access (3PDA) that includes OpenADE and OpenADR. The profile would be developed as a set of requirements around 3PDA. The intent is for ASAP-SG to get the initial legwork done. When gets to maturity then hand off to UtiliSec WG. Will probably be another TF in the UtiliSec WG. How we deal with it in UtiliSec is on the table – how we support other groups, etc.

Have had a couple of select members (Darren, Justin) went out last week to do give preliminary feedback on the requirements doc and give a preview and help groups that lead and participate in feedback. There has not been any formal work started within a formal group. The ASAP-SG team has been in discussions to start profile after handing off AMI Security Profile. Work will commence relatively soon. Near term responsibilities would be being responsive and engaging at an informal level at the OpenADE level. Unless proposed, there are no plans for the WG to start something formal until a mature draft has been developed.

Privacy is assumed to be discussed / addressed as we look at OpenADE.

M: How do you see groups working with NIST, IEC and other efforts? Not always clear.

ASAP-SG is designed to support the SG Security and NIST CSCTG. The AMI Security Profile was pulled into the NIST-IR. There is not a formal agreement with the NIST CSCTG, but the expectation is that all comments from the NIST CSCTG would be resolved by ASAP-SG. Do not see creating parallel paths.

In terms of the SDO’s, SG Security looks to help accelerate the work of SDO’s such as IEC WG 15 by passing work products to them.

The products are offered up to NIST – there are no recommendations as to how the information will be used once they receive it.

## *1.4 OpenADE Security (Steve)*

Overview of OpenADE authorization (refer to requirements document). Steps required to grant access – the utility doesn’t have to have the 3$^{rd}$ party password and vice-versa.

On the utility website the user grants access to the third party. The utility generates a token that becomes associated with the relationship that allows data access to be granted.

M: How much of the OpenADE spec getting into issues of the interface requirements – such as how information is presented vs. the machine-to-machine interface?

The goal is to fully define the machine-to-machine interface. But also want to make recommendations guidelines about user interface. Trying not to define one-to-one interfaces with custom definitions. The goal is to have a common machine-to-machine interface, but not trying to do GUI-interface definitions. Would make a requirement to show user list of third parties that have access, but not how it looks.

The 3PDA will also include OpenADR, from OpenADE's perspective will

The best way to do is to be minimally

There will be additional data elements that 3rd parties and consumers will want to share; but can add additional capability in future versions using the same mechanism.

M: Is this OpenADE 1 or OpenADE 2? Is this for 3rd party to get data from utility, or in version 2 will have capability for utility to get information from 3rd party.

Can add capability in 2.0. See this to be bi-directional, but have separate authorization means.

M: Understand that the generator of the token is the service provider whether it is the utility or the third party.

A request can also be rejected before a token is created.

M: There are devices that sit in customers home that can poll customer data provide to third party. Devices can pull information at faster rates than an AMI system can.

M: There is a proof by example that can authenticate a device from utility.

M: How does this work with demand response? Could this be done through Google for example?

- Yes, depending on configuration.

M: ADE could be the interface for demand response in the future.

M: From security point of view, really need to know what the other use cases are going to be. We don't know what it is really going to look like.

Darren: We fully recognized that if develop third party security profile that it is likely to change, extend, and evolve as the space evolves. We will not have the luxury of time to wait and see what it will be. We should not let it stop us based on our understanding at this time.

M: Just identifying the use cases can help us develop the security. There are some issues that will be different on the different use cases.

Dave: Want to work with security folks to help define the use cases. There are currently four use cases.

Darren: There are several organizational things that we need to look at as we move forward. Don't know if it will be the formation of a security TF, joint TF, etc.

Dave: This work is being done in conjunction with NIST PAP 10 – supplying them with information.

# 2.0 Working Group Issues

## *2.1 Logistics and Process*

### 2.1.1 Teleconference Schedule

Mondays at 2:00 PM Eastern (current day and time is set to align with NIST CSCTG and be able to respond to things addressed on their Monday, 11 AM Eastern teleconference)

- Nov 2
- Nov 16
- Nov 30
- Dec 14

**Next face-to-face**: Jan 18-21st FPL, Juno Beach, FL. Fly into West Palm (There will be special hotel rates)

### 2.1.2 Survey Monkey

Preview:
http://www.surveymonkey.com/s.aspx?PREVIEW_MODE=DO_NOT_USE_THIS_LINK_FOR_COLLECTION&sm=xRr5ErPEgdxo8sY%2bJB1RjV2VL55JYFA9Zsxvw0PyVfI%3d

Note:
There has to be a named chair, vice-chair and secretary. There has to be at least one utility in either the chair or vice-chair role and the other has to be non-chair. The secretary role does not have restrictions.

### 2.1.3 Voting Process (SG Systems)

http://osgug.ucaiug.org/sgsystems/Pages/Voting%20Ballots.aspx

Voting would be blind until the voting window has closed to avoid influencing votes.

There needs to be a review of the votes after the closing period to make sure persons from more than one company do not cast a vote or validate other balloting policies.

May need to keep a registrar of members allowed to vote, identify company association, etc.

**ACTION ITEM:** Darren to follow-up to determine if OpenSG if corporate restriction is to be enforced across all of OpenSG working groups.

## *2.2 Working Group Obligations*

The group has obligations to maintain to be a working group.

**Charter** – can be as simple as a one page PowerPoint. Developed at summer face-to-face at AEP. In the time since, suspect we need to put in voting procedures, who participates, requirements for task forces. Chair looking for help with getting charter finalized.

**ACTION ITEM**: Brian Smith, Tom Overman and John Lilley to work on Charter.

**Project Schedule** – to be developed. Dates coming up with the NIST-IR 763. Two more versions coming out: draft in December and final revision in March. We want to feed into the NIST effort.

C: Do we want to shape our work around the NIST timeline? As a note, the ASAP-SG team is going to hand off the AMI Security Profile to the SG Security.

**ACTION ITEM**: Darren to find out from Annabelle (NIST) the December date that NIST would need deliverables in by for consideration.

C: Would like to get the AMI Security Profile to the 1.0 status by December, otherwise would have to try and get it in by the final NIST-IR in March.

Other things that need to be covered are **Monthly Status**, **Schedule Meetings**, **Sub-groups** (i.e., Task Forces) and **Constitution**.

# 3.0 Topics

**Action Item**: Establish parking lot document for potential projects that

- Prioritization mechanisms -

# 4.0 External Engagement

## *4.1 NIST*

**PAP's –** There is a concern that security issues are coming up and there is not a mechanism to address the issues. Or if there is a business impact of what is being decided in those meetings.

M: Think that working group chairs should get together and address with a common voice concerns with NIST PAPS.

**Action Item**: Darren to follow up at OpenSG level about how to address interfacing with NIST PAPs.

**CSCTG –** Currently has been open exchange with CSCTG and SG Security. A lot of same suspects in the same groups in leadership roles. Members of ASAP-SG are heavily involved with both groups.

### *4.2 NAESB*

NAESB has a security group and standards group. Security group hasn't done so much yet. Wayne Longcore will reach out to security group and see how to setup a liaison status. Matt Carpenter has met with the head of NAESB security and can help.

### *4.3 IEC Technical Committee (TC) 57 Working Group (WG) 15*

IEC is working on drafting standards for key management. This group could provide input.

**Parking Lot**: Key management support for IEC WG 15.

### *4.4 OASIS*

OASIS has a number of standards in regards to web security.

**Action Item:** Wayne Longcore to get in touch with OASIS to develop security liaison status.

### *4.5 NERC Interoperability Taskforce*

Sandy Bacik to serve as liaison for group.

### *4.6 IEEE 2030*

Gary Finco to serve as informal liaison.

### *4.7 IEC WG 14*

Greg Robinson is chair.

## 5.0 ASAP-SG

### *5.1 Intellectual Property*

Deliverables to be posted under smartgridipedia.org with Creative Commons Attribution 3.0.

**Action Item**: Bobby to create location on www.SmartGridipedia.org for SG Security work.

### *5.2 Future Planning*

- Third Party Data Access Security Profile

To be effective need capability to form ListServs/reflectors as needed.

**Action Item**: Bobby to have third party data access security listserv created.

- Network Type Security Profile – network type (mesh, star (tower), or power line) make a difference in security. Between the aggregation point to the meter. Security considerations for each of the topology.
- Distribution Automation Security Profile
- [nominations] – SynchroPhasor Measurement, Transmission Substation Automation (separate from DA)
- Work flow process
    - Deliverable hand-off
    - Review/comment
    - Prioritization/schedule

# 6.0 AMI Security Profile

## *6.1 Update*

Controls from profile originated in the DHS Systems Catalog and are mapped to the AMI space. Many of the controls are organizational in nature, but not specific to technology. Organizational controls have been pulled out and aggregating those into security blueprint document. The team has put most effort into AMI Security Profile and Strategy and Guiding Principles.

One primary purpose of the security profile is to serve as RFP process between utilities and vendors.

The document has the definition of what each of the deliverables are for the blueprint and security profile.

Take stakeholder needs to be taken into consideration; Discussion of overall objectives for security, and list of principles. The target audience is likely the C-level or just below the C-level document.

AMI Security Profile – presented to SG Security.

First public draft release 9/18/09, sent to Usability Analysis team for recommendation and feedback. Review of revision history and changes. Review of document contents. The Domain Analysis section walks through the process of what should be included and required – can see this being updated more. The linkage between domain analysis and recommended controls needs more clarity. DHS updated the security catalog. This guidance is based on the January 2008 DHS catalog.

New controls were added with the “ASAP” prefix if was not based in the DHS control.

All the work will be fed to NIST.

# 7.0 Security Profile Blueprint

## *7.1 Goals/Direction*

ASAP-SG is largely about creating profiles. We may do some future work to expand it to provide guidance for those adapting profiles in various ways. Because it's mostly about creating profiles, we've felt less pressured to get it out to the community as early as the AMI security profile - the latter likely being of much broader interest and applicability.

# 7.0 Strategy & Guiding Principles

## *7.1Review*

James Ivers walk through the Strategy and Guiding Principles – serves as introduction to the smart grid security work, what team was trying to accomplish, what not trying to accomplish, talks about how deliverables fit together, who the intended audience is, etc. This is an evolving document. We'll continue to update it as we make progress and capture new insights. It will be revisited after each other deliverable.

# 8.0 Joint Meeting – AMI Network and SG Security (Matt Gilmore)

NIST PAPs 1 and 2 are being evaluated by group. AMI Network is under SG Communications. Looking at several categories based on things such as meter reads, load management, service switch, etc. Group is discussing PHEVs. Want to make sure not duplicating efforts between groups.

Can SG Security provide security requirements to the AMI Network group so that can use. The AMI Security Profile will be sent to the AMI Network group.

Darren: it may be difficult to pull out the communications guidance. If looking for guidance that has been endorsed and approved, then would have to look at last year's AMI-SEC Security Specification Requirements. Think that ASAP-SG will not change too much between now and when it is approved, and AMI Network will have to take with caveat that it has not been approved by group. The SG Security looking to get AMI Security profile to 1.0 status before the NIST December NIST-IR draft date for use by NIST. The AMI Security profile was not based on the AMI SSR.

Using the AMI SSR 1.01, it is difficult to find controls specified around a specific components – it requires additional work. Recommend using the elements shown in figure 3 – AMI Logical Architecture View of the AMI Security Profile. The table is a good reference for mapping components to security controls.

# 9.0 SG Security – ASAP-SG deliverable discussion

One of the goals of the ASAP-SG AMI Security Profile is to make the requirements provided in the AMI SSR from last year more approachable. Currently the controls are heavy in that everything (controls) applies to everything (components). We really wanted to engage the community in this process. To do this, early on we formed up a team lead by Daniel Thanos, a usability analysis team to do a thorough

review of the documentation from the perspective of the consumers of the document. Version 0.46 was reviewed by the UA team and a preliminary report was submitted to the ASAP-SG Architecture team. ASAP-SG used the report to make changes and address issues/concerns.

## *9.1 Usability Analysis Report (Daniel Thanos)*

Thanks to the ASAP-SG team. There is an opinion that all the controls cannot apply to all the components. There is suggestion to have security levels assigned to controls – to allow for legacy equipment and mitigating standards (FIPS 140 standards as an example). A reference model/architecture on actual devices to show how maps to controls and function. Guiding Criteria of the document describes the problems that have historically existed in the past, and why it is important to apply controls at a granular level to components and systems with justification; and why the recommendations are made.

The team made some usability analysis points. Traceability to tie controls based on impact and use cases. In having to deal with management, they will want to understand why control is recommended and increase of cost is necessary. Component-wise controls – there appeared to be too many things that applied to everything. Every component did not provide the same function as a larger system. Requirement types – since security is a process and technology there is confusion between what needs to be done through a process and what is done by technology. The NERC CIP is an example that can be confusing. Having guidance and clear segmentation between requirement types. Security Levels – controls should have levels that can be a benchmark to spur the industry to be better. DIACAP is shown as an example. The team is not endorsing any security levels. Examples could be level of encryption. Reference model and implementation – think that one of most important thing for the SG Security group would be to develop a good reference model. Further considerations – federation of interoperability (e.g., intersystem commands); focus on resiliency – such as detect, respond and restore) – have to assume that we are having breaches, incidents – consider how to respond, restore, etc. Not sure if these should be handled in the current version, but should be taken in consideration.

**ACTION ITEM**: Post UA document to the SG Security Group.

## *9.2 Review of ASAP-SG Response (ASAP-SG)*

Darren to walk through the UA Document to address ASAP-SG's response; would like to open up to general discussion after the walkthrough.

There is a gap in the traceability that needs to be closed within the document. The team attempted to provide as much traceability as possible. Component-wise controls – we expect feedback from the community to define as part of the process on how might be done. Requirement types – attempted to address in v 0.48 and identify controls that were strictly organizational in nature and plan to integrate into security profile blueprint. Evidence – agreed with comment, but didn't feel that ASAP-SG team was equipped to put adequate guidance within given timeframe. Think it best to put forth to the SG Security team (AMI-SEC). Have a vested interest in getting the document pushed out to the NIST-IR. Security levels – we understood the comment, but the ASAP-SG team was trying to create baseline level of

controls, so distinguishing between high-level verses low-level controls was not made. Think this would involve quite a few discussions and work to do this. Reference model and implementation – ASAP-SG is not the right body to create this. The AMI-SEC TF community may be the better place, and better yet, a vendors could provide their architecture as a case. The team received other comments from other groups that received the document and tried to address those concerns also. One of the bigger concerns was in DHS-2.8.7 Boundary Protection. There was a recommendation to do only one way communications into the HAN. Many recommendations from above said that the guidance would be summarily rejected, due to the need for two directional communications into the HAN. The Open HAN SRS specifies that two-way communication is required. In Texas it is law to allow two way communications for establishing demand response. Therefore, the team overhauled the wording. Two way communications is a risk and that boundary protection should be established in key areas to contain incidence – between Utility-WAN, WAN-NAN, and NAN-HAN. There are some compensating controls that need to be developed to manage the egress back into the meter.

M: A lot of standards have a base. And then optional standards for additional capability. Could do something for one-way communication and an extension for two-way communication?

M: Comment: Implemented two systems that started out one way, and soon became two-way. Because of technology changes, if only one way communications exist, then it will kill us long term. Think that it is a bigger risk to have one way communications than having the two-way with risk of being hacked.

C: This organization is part of the OpenSG. They approve or disapprove what is produced by this group. The OpenSG has made it clear that SG Security is to provide guidance to the home with two-way communications.

M: There are utility installed interrupters. In doing a field survey on interrupters more than 40% had been disabled. There was no way to query or know that they have been shut off. There are some devices that are going to only sense – one level of security. There may be other sensors that relay messages from other sensors. There are another type that can sense, relay and control that need a separate level on control. People can do more damage to a pure sensor than just relays and controls.

M: Understand a need for two-way communication. Is there an alternative to having the communication going into the home through one path and then out through a separate path?

C: There is nothing that precludes that in the current document. But this scenario is out of scope for a channel not in control by the utility or third party.

C: Other feedback/comments/concerns? Structure? Content?

M: What is next? In regard to NIST are these changes going to be submitted?

C: In terms of the NIST, need to close loop with Annabelle when would absolutely need to provide content into the NIST-IR. We would like to get the document to 1.0 status by the December deadline. We would need to get all comments identified and resolved within about 1 month; and that is if it passes on the first vote. As a reminder the document last year did not pass on the first vote.

M: In GridWeek talked about the best practices, messages in flight. As go through service definition artifacts and do implementations. In looking in WS Security can encrypt certain nodes and several flavors of encryption. When building out example implementations how would be addressed? And if not available would be a second best choice? As of today how would we address that?

C: What is the request?

M: The request is to get guidance in looking at data at rest, data in process and data in flight.

C: Specifically on of the encryption being looked at is ECC. Does making ad-hoc comments covered in another document.

M: In procurement language document then make reference to other documents. This may be a means to handle this.

M: Are looking to have reference to standards so that development can be based on standards.

M: Don't think we should pick winners and losers.

C: Don't mind point to a reference body such as NIST or NSA, but explicitly referencing a specific technology may not be the best practice for this group. But could point to other documents as a reference.

M: If a way to categorize security technologies then would be good. A way to reference something or point to another document would be good. And rate the categories.

C: Would be dangerous to say x is good and y is bad. Need to steer clear of passing judgment on specific technologies.

C: We need more activities link the joint working sessions.

M: What may be able to provide is guidance on what encryption types to use base on use. Such as for high bandwidth vs. low bandwidth, high processing vs. low processing.

C: NSA has this guidance.

## *9.3 Process Moving Forward*

Kay Clinard: Work doing here needs to be linked into a NIST PAP. Because they move up and get into NIST and then voted on. The SGIP panel and SGIPGB (self nominated). Encourage all companies to join SGIP. Have a chance to have a voice. Go to NIST website and register. There will be webinars so that small companies attend. They have the rules posted on the website for voting. In the long term, the smart grid will incorporate all the things under discussion.

---

VC: Have questions that we think need answering.

M: Think of having help desk functionality for issue tracking system.

C: Get questions identified in the technical distribution list.

M: Can convert questions into a FAQ.

C: Created the technical email list because technical conversations took over. UtiliSec technical has been notably quite since we formed it. Not sure what it is about lists with over 200 prescribers to voice our opinion on every technical matter. We've got a venue for these technical conversations let's use it.

M: Asked to send feedback to UA technical committee? Should do this on the technical email?

C: For clarification, the UA technical discussions should be dealt with on the UA listserv. But for general comments then should be addressed in the UtiliSec technical. If have technical comment/concern on current document that needs more discussion and debate then bring up in the UtiliSec technical.

**ACTION ITEM**: Make sure have UA list on the SharePoint site.

---

## *9.4 Process for Review, Revision Convergence and Vote*

Technical issues – each person can have a vote; in other cases a company only has one vote.

**ACTION ITEM**: Darren to follow up with policies and principles for voting process, should voting be at corporate level.

**ACTION ITEM**: Bobby, aggregate eligible voting members list.

---

Motion made to **qualify for vote that prior to voting must have been on the record to have attended 3 out of 5 meetings either by phone or face-to-face**.

Motion seconded.

Opened for discussion.

No discussion.

Call for vote.

All "yes" votes, No "no" votes.

---

Motion made to **not count abstained votes in the total for determining the 2/3rds majority**.

Motion seconded.

Opened for discussion.

No discussion.

Call for vote.

All "yes" votes, No "no" votes.

---

M: Is quorum needed to pass a vote? And what defines a quorum?

M: I think a quorum is needed. A quorum by OpenSG is 50% of eligible voters.

C: **Will state that a quorum is 50% of eligible voters.**

C: **Comments made to the document must be addressed with a proposed resolution.**

C: **Process will be to identify the section, page number and specific text to be**

**Action Item**: Darren or Bobby: Put together a spreadsheet to distribute to the task force so that the UA Team can aggregate comments and proposed changes.

C: **AMI-TF will vote on version 0.49 of the AMI Security Profile document**.

C: **We will accept comments from NIST before November 13th.**

## Balloting Schedule for AMI Security Profile

- October 30 - ASAP-SG delivers v 0.49
- November 13 - All proposed changes due
- November 16 - Teleconference/Review
- November 27 - Edit to roll in all changes (all changes finalized)
- December 2 - AMI-SEC TF Publishes 0.9
- December 3 - Voting begins
- December 9 - Vote by AMI-SEC TF (voting process ends)
- December 10 - Vote by OpenSG Technical Committee
- December 11 - for version 1.0 tentative due date to NIST.

C: At this point the ASAP-SG is handing off this version of the AMI Security Profile v 0.48. From this point the thought is that AMI-SEC will revise beyond this.

# 10.0 Other

## *10.1 INL AMI Wireless Procurement Language Document*

This work was a follow on to the ASAP (AMI Security Acceleration Project) of last year.

Gary Finco: The comments have been collected and put into a spreadsheet. Would like to get a modified version out by next month. Would like to have comments in by October 30th. Comments can be sent directly to Gary, Darren or the UtiliSec ListServ.

## *10.2 Formation of new TF*

Review of rules for starting a new task force.

Joe Hughes – Security issues surrounding IP. Relates to NIST PAP 1. Could form task force around this.

Doug Houseman – notice there is a lot of interest developing around privacy in smart grid and smart grid data.