

ASAP-SG

From SmartGridiPedia

Advanced Security Acceleration Project for the Smart Grid

Link: [AMI Security Profile v2.0](#)

The AMI Security Profile was developed by the ASAP-SG team in order to accelerate the development of security requirements and standards. This work product has been accepted and used by NIST Cyber Security Working Group and the AMI-SEC Task Force within the UCAIug.

Link: [ASAP-SG Third Party Data Access Security Profile v1.0](#)

The Third Party Data Access Security Profile was developed by the ASAP-SG team in order to accelerate the development of security requirements and standards. This document delineates the security requirements for individuals, utilities, and vendors participating in a three-way relationship that involves the ownership and handling of sensitive data. Specifically this document is aimed at the smart grid environment, and is intended to address the concerns of electric utility customers who want to allow value added service providers to access electric usage data that is in the custody of the customer's utility. Other three-way data sharing scenarios may also be addressed using this profile, as the roles of the three parties have been abstracted in such a way as to support mapping to different environments.

Link: [ASAP-SG Distribution Management Security Profile v1.0](#)

The Distribution Management Security Profile was developed by the ASAP-SG team in order to accelerate the development of security requirements and standards. This document defines security requirements for automated distribution management (DM) functions in a smart grid environment, including steady state operations and optimization. This document addresses concerns related to using communications and automation in field equipment that controls the configuration and operation of the electric distribution system. Other electric system operation scenarios may also be addressed using this profile, as the various roles defined herein have been abstracted in such a way as to support mapping to different environments.

Link: [ASAP-SG Wide-Area Monitoring, Protection, and Control \(Synchrophasor\) Security Profile \(Draft\) v0.08](#)

The Wide-Area Monitoring, Protection, and Control (WAMPAC) Security Profile was developed by the ASAP-SG team in order to accelerate the development of security requirements and standards. This document defines security requirements for wide-area monitoring, protection, and control of the electric grid, specifically leveraging synchrophasor technology. This profile addresses security concerns associated with the use of phasor measurements in electric system operational decisions, whether these decisions are made off-line, real-time but manually, or through automated processes. The recommendations made herein are based on stated system architectural and functional assumptions, and

offer a singular security baseline for overall use of synchrophasor technology with tailored subsets of recommendations where variations in system deployment or usage occur.

Link: [ASAP-SG Substation Automation Security Profile \(Draft\) v0.15](#)

The Substation Automation Security Profile was developed by the ASAP-SG team in order to accelerate the development of security requirements and standards. This document defines security requirements for electric grid substation automation technology. The profile addresses security concerns associated with automated and manual interaction in support of system protection (inter and intra-substation), system control (local and remote), system optimization (e.g., voltage and reactive power), and system monitoring (i.e., equipment health) performed by equipment located in transmission and distribution substations.

Link: [ASAP-SG Security Profile Blueprint v1.0](#)

The Smart Grid Security Profile Blueprint provides the electric utility industry along with supporting vendor communities and other stakeholders a framework, set of tools, and method to create and customize Smart Grid domain-specific security profiles. These security profiles specify security requirements that should be applied to the procurement, implementation, and configuration of Smart Grid systems.

The primary audience of the Blueprint is any organization attempting to create a new security profile or customize an existing security profile; therefore the document is written for security architects from utilities, vendors, and system integrators that have experience with utility security. Other stakeholders, such as vendors, can use this document to understand how a particular set of security controls was selected as part of a particular security profile. The Blueprint is intended to produce requirements that are technology-specific but vendor-agnostic, and does this by defining a process for creating a security profile. This process includes the delineation of profile scope, creation of a logical reference architecture, definition of objectives for secure operation, performance of a failure analysis, recommendation of security controls, and validation of criteria for satisfaction of requirements.

Link: [How a Utility Can Use ASAP-SG Security Profiles \(White Paper\)](#)

This document describes several different ways that ASAP-SG security profiles can be used to improve the security of smart grid systems. We assume that the business decision to create or modernize a system has already been made and that procurement will be an important element of the project. We do not assume a particular procurement process or how project responsibilities may be distributed across particular organizational units. Instead, we focus our discussion on elements that are integral to any smart grid project—elements like sets of requirements, designs, and procured or internally developed equipment or systems—and how a security profile can be used (for example) to help create, test, or configure these elements.

Retrieved from "<http://10.0.200.23:8080/index.php/ASAP-SG>"

- This page was last modified on 27 November 2012, at 18:07.
- Content is available under Attribution 3.0 Unported.