Project	ZigBee Alliance		
Title	ZigBee Response to PAP 18		
Date Submitted	1/27/12		
Source	[Tobin Richardson] [ZigBee Alliance] [2400 Camino Ramon, Suite 375 San Ramon, CA 94583]	Voice: Fax: E-mail:	[+1.916.801.5810] [+1.925.886.3850] [trichardson@zigbee.org]
Re:	Smart Grid Interoperability Panel's (SGIP) Priority Action Plan (PAP) 18 Recommendations and Requirements for ZigBee		
Abstract	This document responds to the PAP 18 SEP 1.x to SEP 2.0 Transition and Coexistence White Paper.		
Purpose	The recommendations in this document would need to be implemented in a future revision of the Smart Energy 1.x and 2.0 specifications.		
Notice	This document has been prepared to assist the ZigBee Alliance. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.		
Release	The contributor acknowledges and accepts that this contribution will be posted in the member area of the ZigBee web site.		

Abstract

This document provides recommended resolutions to the NIST Priority Action Plan (PAP) 18 Workgroup on Smart Energy Profile (SEP) 1.x to SEP 2.0 Transition and Coexistence White Paper. These recommendations provide guidance on how to proceed with updates to the Smart Energy specification for the ZigBee Smart Energy Workgroup and also recommend the ZigBee Alliance develop a separate document on Guidelines and Recommendations for Implementation and Coexistence.

Introduction

As part of the NIST and Smart Grid Interoperability Panel process, PAP 18 was formed to address the migration and coexistence of SEP 1.x and SEP 2.0. Because of architectural changes and feature upgrades, SEP 1.x and SEP 2.0 are not over the air compatible. Because many meters have been or are being deployed with SEP 1.x, it was requested that a migration and coexistence strategy to outline the requirements and best practices be completed. PAP 18 completed this work and the White Paper created is located at:
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SEPTransitionAndCoexistenceWP

This document extracts the specific recommendation and requirements from the PAP 18 White Paper and provides specific ZigBee Alliance responses. These responses would then need to be incorporated into either an update to the Smart Energy Profile, or a separate document on Guidelines and Recommendations for Implementation and Coexistence.

Note that all recommendation or Best Practices from PAP 18 are included below for completeness. Those recommendations not directed at the ZigBee Alliance are so indicated.

This document commits to developing the following documents that are noted in various responses below:

a. Update to Smart Energy 1.x Specification
b. Update to Smart Energy Over the Air Upgrade Cluster
c. Requirements for Inclusion in Smart Energy 2 Specification
d. Requirements and specification for Dual Mode devices
e. ZigBee Application Level Gateway specification, test plan and PICS
f. Best Practices and Guidelines for Deploying SEP 2.0 on existing ESI devices
g. Best Practices and Guidelines for Deploying SEP 2.0 on existing HAN devices

The specific timeline for release of an update to these documents including these recommendations is in the next several months, and at least coincident with the release of finalized SEP 2.0 documents and specifications.

Among contributors, it is expected the following ZigBee work groups, sub-groups and special interest groups will contribute to the following recommendations.

- Smart Energy Working Group
- Smart Energy Marketing Vertical
- ZIP – ZigBee IP
- Core Stack Group
- Gateway Working Group
- Security Working Group
- Australia SIG
- Europe SIG

Specific Concerns or Recommendations Notes

This section is a placeholder for incorporation specific concerns and other related notes.

- Until the specification is complete, the extent of SEP 2.0 compatibility will not be fully understood.

ZigBee Alliance Requirements

SEP 1.x to SEP 2.0 Migration-Specific Requirements

REQ.ZA.1 Market participants (e.g. Utilities, Manufactures, Regulatory Authorities, etc.) shall determine (e.g. through the ZigBee Alliance) the minimum set of SEP 2.0 features required to implement the basic functionality of a Utility ESI and Metering server.

ZigBee Alliance Response:

As part of the SEP 2.0 efforts, a separate document will be developed specifying the minimum SEP 2.0 application and IP stack functionality for ESI and Metering function sets within a device. This will be developed in conjunction with stack providers and device manufacturers to reflect the constraints of the existing deployed product, SEP 2.0 early implementations and the system topologies outlined in the PAP 18 white paper. This will be reviewed later with the other market participants noted in the requirement.

REQ.ZA.2 The ZigBee Alliance shall determine the minimum ZigBee IP stack necessary to support the minimum set of SEP 2.0 features required to implement the basic functionality of a Utility ESI. This will determine which Upgradeable SEP 1.x Utility ESIs will support firmware migration.

ZigBee Alliance Response:

As part of the SEP 2.0 efforts, a separate document will be developed specifying the minimum SEP 2.0 application and IP stack functionality for ESI and Metering function sets within a device. This will be developed in conjunction with stack providers and device manufacturers to reflect

the constraints of the existing deployed product, SEP 2.0 early implementations and the system topologies outlined in the PAP 18 white paper. This will be reviewed later with the other market participants noted in the requirement.

REQ.ZA.3 A procedure shall be defined for replacing SEP 1.x security credentials with SEP 2.0 security credentials on a deployed device.

ZigBee Alliance Response:

ZigBee Alliance will review and as appropriate update the SEP 1.1 OTA cluster, PICS and test plan will be done to validate passing a block of data suitable for SEP 2.0 security material. Test cases will be included to validate this functionality on devices. The update will include an OTA migration procedure best practices to minimize the risk associated with performing this procedure.

REQ.ZA.4 SEP 1.x HAN devices shall have the ability to perform a firmware migration (e.g., OTA, manual, etc.).

ZigBee Alliance Response:

The ZigBee Alliance believes it partially meets this requirement. The Alliance does not necessarily agree this will be a requirement for all devices. There are three logical types of devices relevant here:

(1) OTA – those devices that have included the OTA option, and have tested to it (OTA Cluster);

(2) Vendor-specific or manual – The Alliance can not control, so can not verify it will or will not be capable of upgrading to SEP 2.0;

(3) Non-upgradable devices. No firmware upgrade – would need a gateway or other implied handling. Some product manufacturers have made the decision that there is a market for these types of devices. The SEP 1.1 specification added OTA firmware migration as a feature. This feature is optional on devices and manufacturers may choose other methods for upgrading devices such as manual upgrades.

Application Layer Gateway (ALG) Specific Requirements

REQ.GW.1 ZigBee Alliance members shall determine how an ALG will bi-directionally translate between the SEP 1.x and SEP 2.0 application layers. The translation shall be based on the SEP 1.x Clusters. Note: this will enable device interoperability.

ZigBee Alliance Response:
The ZigBee Alliance will complete a mapping of the SEP 1.x to the SEP 2.0 data model and include behavior rules for fields present or not present to allow a bi-directional mapping in the ALG for the scenarios outlined in the white paper. This will be captured in the ALG specification which will also include any other network or functional requirements.

REQ.GW.2 When the Utility ESI (e.g. Smart Meter) SEP firmware is migrated to SEP 2.0, an ALG equipped to translate between SEP 2.0 and SEP 1.x networks shall enable existing SEP 1.x devices to continue to be active and function.

ZigBee Alliance Response:
The ZigBee Alliance will complete a mapping of the SEP 1.x to the SEP 2.0 data model and include behavior rules for fields present or not present to allow a bi-directional mapping in the ALG for the scenarios outlined in the white paper. This will be captured in the ALG specification which will also include any other network or functional requirements.

REQ.GW.3 The Registration process for the ALG and HAN devices that are Commissioned to the ALG shall be clearly defined and communicated to the Consumer.

ZigBee Alliance Response:
The registration process will be captured as a requirement in the ZigBee development of an ALG specification. This specification will detail the behavior and requirements for an ALG, and will be developed along with the appropriate test plan and PICS to allow certification of such devices. The ZigBee Alliance assumes that the service provider will manage appropriate consumer communication, and this point will be captured in the best practices and guidelines document.

Dual Mode Home Area Network (HAN) Device Requirements

REQ.DM.1 Dual Mode devices shall be capable (e.g. automatically, manually, etc.) of switching from one SEP firmware to another.

ZigBee Alliance Response:

The ZigBee Alliance will develop specific requirements and behaviors for dual mode devices to allow these devices to be tested and certified. This will provide specific requirements on automatically or manually being directed to switch between firmware images. How switching is accomplished is up to the manufacturer. These requirements will be captured as a stand-alone specification that defines the requirements and behavior of dual mode devices.

REQ.DM.2 A Dual Mode device shall have a method to detect what SEP specification the ESI is using and connect to the HAN using the appropriate SEP firmware.

ZigBee Alliance Response:

The ZigBee Alliance will develop specific requirements and behaviors for dual mode devices to allow these devices to be tested and certified.

Manufacturer and Utility Requirements

SEP 1.x to SEP 2.0 Migration Specific Requirements

REQ.SEP.1 Manufacturers shall determine and communicate to the Customer and other market participants if their SEP 1.x device will support the identified minimum set of SEP 2.0 features.

ZigBee Alliance Response:

The ZigBee Alliance will develop a document of Best Practices and Guidelines for migrating to SEP 2.0 for existing SEP 1.x devices and currently has a certification and logo program which allows appropriate labeling of devices. Each manufacturer may have different versions of hardware and software on installed SEP 1.x devices that must be evaluated for SEP 2.0 capability.

REQ.SEP.2 Manufacturers shall clearly communicate to the Customer and other market participants which SEP applications their device supports.

ZigBee Alliance Response:

The ZigBee Alliance will develop a document of Best Practices and Guidelines for migrating to SEP 2.0 for existing SEP 1.x devices and currently has a certification and logo program which allows appropriate labeling of devices. Each manufacturer may have different versions of hardware and software on installed SEP 1.x devices that must be evaluated for SEP 2.0 capability.

REQ.SEP.3 Manufacturers shall clearly communicate to the Customer and other market participants the migration path and the capability of their devices to migrate from SEP 1.x to SEP 2.0 if supported.

ZigBee Alliance Response:

In order to support this requirement, the ZigBee Alliance will specify that a vendor is to clearly define the capabilities of the device to migrate from SEP 1.x to SEP 2.0, and what the procedure is. The options for devices will also be communicated to other market participants. This will be enabled by the certification and logo program developed by the ZQG and ZigBee Marketing Steering Committee.

REQ.SEP.4 Manufacturers shall communicate to the Customer and other market participants how to obtain and install SEP 2.0 firmware for that Manufacturer's devices if supported.

ZigBee Alliance Response:

In order to support this requirement, the ZigBee Alliance will specify that a vendor is to clearly define and identify what SEP version a device will support, and that vendors shall identify (if supported) firmware upgrade procedures to customers (end users, utilities, etc.). The options for devices will also be communicated to other market participants. This will be enabled by the certification and logo program developed by the ZQG and ZigBee Marketing Steering Committee.

REQ.SEP.5 The requirements for obtaining SEP 2.0 security credentials and replacing SEP 1.x security credentials with SEP 2.0 security credentials shall be communicated to market participants, if supported.

ZigBee Alliance Response:

In order to support this requirement, the ZigBee Alliance will specify that a vendor is to clearly define and identify which SEP versions a device will support and how new security credentials can be obtained. The options for updating devices security credentials will also be communicated to other market participants. This will be enabled by the certification and logo program developed by the ZQG and ZigBee Marketing Steering Committee.

REQ.SEP.6 SEP 2.0 security credentials for each HAN device in the field shall be available, assigned and downloaded to a unique HAN device based on its MAC address.

ZigBee Alliance Response:

Assumes the HAN device in question has the capability to be upgraded. The update to the ZigBee Over the Air Cluster will address how security credentials shall be validated by a device to ensure it is for the proper device.

REQ.SEP.7 Manufacturers shall ensure that their HAN devices implement the procedure for replacing SEP 1.x security credentials with SEP 2.0 security credentials on deployed devices.

ZigBee Alliance Response:

The update to the ZigBee Over the Air Cluster will include test procedures and PICS requirements to validate HAN devices can replace SEP 1.x security credentials with SEP 2.0 security credentials if this material is not preinstalled.

REQ.SEP.8 Where applicable, the over the air (OTA) upgrade process for HAN Devices to migrate from SEP 1.x to SEP 2.0 shall be clearly defined and communicated.

ZigBee Alliance Response:

While the ZigBee over the air cluster defines the device-to-device communications within the ZigBee network, a separate appendix will be developed to more clearly define the system level process and recommendations for the upgrade. This will be included in the update to the OTA cluster document.

REQ.SEP.9 Utilities shall communicate how to Register HAN devices to the Utility ESI based on what SEP firmware is in the Utility ESI (e.g., Smart Meter).

ZigBee Alliance Response:

This requirement is not a ZigBee Alliance action item but should be aided by the implementation guidelines document. The working understanding is that there will be networks with mixed nodes on them based on having an ALG in the network, but the Utility ESI is used as the connection to the utility for determining the registration method.

Application Layer Gateway (ALG) Specific Requirements

REQ.GW.4 The networks and applications that the ALG supports shall be clearly communicated to the Customer.

ZigBee Alliance Response:
This requirement will be captured as part of the development of the ALG specification. The specification detailing the behavior and requirements for an ALG will be developed along with the appropriate test plan and PICS to allow certification of such devices. The ZQG and ZigBee Marketing Steering Committee will have the action on specifying logos and markings to clearly identify what is supported on the device. The ZigBee Alliance assumes that this requirement does not mandate the ALG to have broadband backhaul to function.

REQ.GW.5 It shall be clearly communicated to the Customer when the use of an ALG is required.

ZigBee Alliance Response:

While the ZigBee Alliance ALG specification will define when and how the ALG is used, this is an action for the market participants installing the ALG and not the ZigBee Alliance.

REQ.GW.6 ALGs shall come with clear instructions on how to Register HAN devices to an ALG.

ZigBee Alliance Response:

While the ZigBee Alliance ALG specification will define when and how the ALG is used, this is an action for the market participants installing the ALG and not the ZigBee Alliance. The ALG specification will include a requirement to specify a transport mechanism for communicating credentials to or through the ALG to allow device registration.

REQ.GW.7 ALGs shall provide a method to verify the SEP 2.0 firmware versions and update, if necessary, prior to a SEP 1.x to SEP 2.0 migration.

ZigBee Alliance Response:

The ZigBee Alliance assumes this requirement pertains to HAN devices that are connected to the ALG. The ALG specification will include a mechanism to allow for the ALG to indicate the SEP 2.0 version. The ZigBee Alliance interprets the second part of GW.7 to mean a mechanism is needed to allow the ALG owner to enable automatic upgrades based on the identity of the device. The ALG specification will mandate that a mechanism exist within the ALG to automatically or manually execute SEP 1.x to SEP 2.0 migrations.

REQ.GW.8 An ALG providing translation between SEP 1.x and SEP 2.0 shall provide link layer, application layer and platform security in order to not degrade security for the HAN.

ZigBee Alliance Response:

This requirement will be included in the ALG specification developed. The ZigBee Alliance assumes the requirement is stating that security currently in SEP 1.x and SEP 2.0 shall remain at or above their current levels during operation.

Dual Mode Home Area Network (HAN) Device Requirements

REQ.DM.3 For deployed Dual Mode devices, a method shall be available to verify the SEP 2.0 firmware versions and update if necessary prior to a SEP 1.x to SEP 2.0 migration.

ZigBee Alliance Response:

The Dual Mode device specification will include a mechanism to allow for the Dual Mode device to indicate the SEP 2.0 version. The ZigBee Alliance interprets the second part of DM.3 to mean a mechanism is needed to allow the Dual Mode device owner to enable automatic upgrades. The Dual Mode device specification will mandate that a mechanism exist within the Dual Mode device to automatically or manually execute a SEP 1.x to SEP 2.0 migration.

REQ.DM.4 It shall be clearly communicated to the Customer when a device is Dual Mode and what applications (e.g. SEP 1.x, SEP 2.0, etc.) the device supports.

ZigBee Alliance Response:

This requirement will be included in the specification for Dual Mode devices and ZigBee Alliance Marketing Steering Committee will have the action on clearly identifying the device's behavior.

Best Practices

SEP 1.x to SEP 2.0 Migration

BP.SEP.1 Utility AMI and HAN Management Systems should support SEP 1.x and SEP 2.0 HAN implementations concurrently.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.2 Utility AMI Management Systems should support the ability to perform individual Utility ESI (e.g., Smart Meter) firmware migrations.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.3 A Service Provider's HAN Management Systems should support both SEP 1.x and SEP 2.0 HAN programs.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.4 Utility should supply reasonably sufficient information to the Customer about what SEP firmware is in their Utility ESI (i.e. Smart Meter).

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.5 Customers should be provided with reasonably sufficient information by Utilities, Service Providers, Manufacturers, or Retailers to determine what kind of device(s) (e.g. Dual Mode, ALG, SEP 1.x, SEP 2.0, etc.) will function in their HAN.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.6 Utilities should offer adequate technical support to Customers, Retailers, and Service Providers during a migration to help ensure all migration issues are resolved.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.7 Options supported by Utility and Service Provider for HAN device SEP firmware migration should be presented to the Customer allowing the Customer to choose which option is best for their device.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.8 If a Customer has HAN Devices Registered to the Utility ESI, Utilities should allow the Customer to choose if and when the Utility will perform the Smart Meter SEP firmware migration.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.9 The OTA function should be included in all SEP 1.1/2.0 HAN devices.

ZigBee Alliance Response:

ZigBee Alliance agrees and will include this in best practices document.

BP.SEP.10 If the HAN device SEP firmware is migrated OTA using the Utility AMI system, the Utility should reasonably coordinate the migration with all affected parties (e.g. Customer, Service Provider, Manufacturers, etc.).

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.SEP.11 If the HAN device SEP firmware is migrated OTA using an ALG via the Internet, the Utility/Service Provider should reasonably coordinate the migration with affected parties (e.g. Customer, Manufacturer)

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

Communication of Migration Plans

BP.UtilCom.1 When Utilities develop a migration plan, Utilities should publicly communicate such plan to Service Providers, Retailers, Regulatory Authorities and Manufacturers.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.UtilCom.2 When Utilities develop a migration plan, the Utility should allow reasonably sufficient time in the plan prior to the start of the migration for Service Provider, Retailers, and Manufacturers to prepare for the impact of the migration.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.UtilCom.3 When Utilities develop a migration plan, Utilities should directly communicate such plans to all Customers who have HAN devices, including ALGs, Registered to the Utility ESI, along with the expected date the Customer's Smart Meter SEP firmware will be migrated.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.UtilCom.4 When Utilities communicate their migration plan to Customers, the communication should include the reasonably expected effects of the migration on HAN devices, including ALGs, and any HAN programs (e.g. Utility program, Service Provider Program, EMS, etc.) in which the devices may be participating.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.UtilCom.5 The Utility migration communication sent to Customers should provide the Customer reasonably sufficient information so the Customer may adequately notify their Service Provider in order to maintain the benefits of their HAN program.

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

Manufacturer and Retailer

BP.MR.1 Retailers should offer to bundle ALGs with HAN devices when devices are being sold with a SEP firmware that is incompatible with the SEP firmware in the Utility ESI (e.g., Smart Meter).

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.MR.2 Retailers and Manufacturers should offer HAN devices capable of functioning as an ALG across multiple networks (e.g., other protocols and media).

ZigBee Alliance Response:

This is not a ZigBee Alliance requirement.

BP.MR.3 Existing Registered Dual Mode devices should automatically re-Register after migration with minimal user intervention.

ZigBee Alliance Response:

The ZigBee Alliance will take this recommendation under advisement during the development of the DM specification.

BP.MR.4 ALGs should have the ability to act as an ESI.

ZigBee Alliance Response:

The ZigBee Alliance will take this recommendation under advisement during the development of the ALG specification.

BP.MR.5 ALGs equipped for connection to the Internet should include Router functionality.

ZigBee Alliance Response:

The ZigBee Alliance will take this recommendation under advisement during the development of the ALG specification.

CSWG REVIEW SECTION

ZigBee Response to the PAP 18 Response to CSWG review of the White Paper

The Cyber Security Working Group conducted a review of the PAP 18 white paper (version 1.0) and identified a number of concerns and issued a series of recommendations. The PAP 18 responses to these concerns and recommendations are below. The ZigBee Alliance response to the PAP 18 is included here.

Specifically, the CSWG recommends the following security requirements be included in the SEP 1.x to SEP 2.0 Transition and Coexistence White Paper, or in the subsequent more detailed document:

- Addressing the comments in Table 1 of this review

REF	Reference in White Paper	Comments if NISTIR Requirement Is Not Completely Met	PAP 18 Response	ZigBee Response
1	REQ.ZA.3 A procedure shall be defined for replacing SEP 1.x security credentials with SEP 2.0 security credentials on a deployed device.	The whitepaper requirement does not provide any details on the type or use of the security credentials.	This issue will be referred to the ZigBee Alliance for detailed development of replacement of security credentials.	The ZigBee Alliance agrees and will include these requirements in the upgrade specification.
2	REQ.ZA.4 SEP 1.x HAN devices shall have the ability to perform a firmware migration (e.g., OTA, manual, etc.)	The whitepaper specifies a firmware upgrade but does not identify any security requirements that should be met during the upgrade.	OTA security is being addressed by the ZigBee Alliance through the CSWG review of SEP 1.1. A section dealing specifically with HAN device migration scenarios has been added to the White Paper Appendix to eliminate any ambiguity associated with the process.	The ZigBee Alliance agrees for over the air firmware upgrades there should be specific security requirements and these are included in the OTA specification. For other methods of firmware upgrade ZigBee does not specify requirements.

3	REQ.GW.2 When the Utility ESI (e.g. Smart Meter) SEP firmware is migrated to SEP 2.0, an ALG equipped to translate between SEP 2.0 and SEP 1.x networks shall enable existing SEP 1.x devices to continue to be active and function.	The whitepaper specifies a firmware upgrade but does not identify any security requirements that should be met during the upgrade.	This issue will be referred to the ZigBee Alliance for detailed development of application and physical security requirements for ALGs.	The ZigBee Alliance agrees and this will be addressed in the ALG specification.
4	REQ.DM.1 Dual Mode devices shall be capable (e.g. automatically, manually, etc.) of switching from one SEP firmware to another.	Dual mode devices must include security as part of the switching process itself, but these security requirements are not specified.	This issue will be referred to the ZigBee Alliance for detailed development of security requirements for dual mode devices. Additional information has been added to the White Paper explaining that networks will not be bridged during the switching process of a dual mode device.	The ZigBee Alliance agrees this is an item to be included in the Dual Mode devices specification.
5	REQ.SEP.5 The requirements for obtaining SEP 2.0 security credentials and replacing SEP 1.x security credentials with SEP 2.0 security credentials shall be communicated to market participants, if supported.	The whitepaper requirement does not provide any details on the replacement of the security credentials.	This issue will be referred to the ZigBee Alliance for detailed development for obtaining and replacing security credentials.	The ZigBee Alliance will develop methods for upgrading security credentials. How this is communicated to market participants is not within the ZigBee scope.
6	REQ.SEP.6 SEP 2.0 security credentials for each HAN device in the field shall be available, assigned and downloaded to a unique HAN device based on its MAC address.	The whitepaper requirement does not provide any details on the use of the security credentials.	This issue will be referred to the ZigBee Alliance for detailed development for obtaining and replacing security credentials.	The ZigBee Alliance specification for upgrading devices will include details on how to include new security credentials.

7	REQ.SEP.7 Manufacturers shall ensure that their HAN devices implement the procedure for replacing SEP 1.x security credentials with SEP 2.0 security credentials on deployed devices.	The whitepaper requirement does not provide any details on the security requirements for the manufacturers' procedures for replacing the security credentials.	This issue will be referred to the ZigBee Alliance for detailed development for obtaining and replacing security credentials.	The ZigBee Alliance agrees the specifications developed will include requirements on how to upgrade security credentials. Refer to item G; guidelines for updating existing HAN devices.
8	REQ.SEP.8 Where applicable, the over the air (OTA) upgrade process for HAN Devices to migrate from SEP 1.x to SEP 2.0 shall be clearly defined and communicated.	The whitepaper specifies a firmware upgrade but does not include the security requirements which must be met during the upgrade.	OTA security is being addressed by the ZigBee Alliance through the CSWG review of SEP 1.1. A section dealing specifically with HAN device migration scenarios has been added to the White Paper Appendix to eliminate any ambiguity associated with the process.	The ZigBee Alliance agrees there should be security requirements on how to perform OTA firmware upgrades. These are already included in the SE specification as well as in the OTA specification.
9	REQ.SEP.9 Utilities shall communicate how to Register HAN devices to the Utility ESI based on what SEP firmware is in the Utility ESI (e.g., Smart Meter).	The whitepaper does not include the security requirements which must be met during a change in registration from SEP 1.x to SEP 2.0.	Information on the migration of the Utility ESI and why it is considered out of scope for PAP 18 has been added to a HAN Device Migration section in the White Paper Appendix along with other specific HAN Device migration information.	No specific request of ZigBee Alliance in this comment.

10	REQ.GW.8 An ALG providing translation between SEP 1.x and SEP 2.0 shall provide link layer, application layer and platform security in order to not degrade security for the HAN.	The ALG does not include security requirements for performing translations between SEP 1.x and SEP2.0, other than not "degrading security for the HAN," which is too vague to provide a means for testing these translations.	This issue will be referred to the ZigBee Alliance for detailed development of application and physical security requirements for ALGs.	The ZigBee Alliance agrees that requirements should be included in the ALG specification.

436

437 • Security requirements for the ALG, including the development of key Use Cases

438 o All specification and security related development for Application Layer Gateways is being
439 referred to the ZigBee Alliance. The ALG is the only device envisioned by the White Paper to
440 bridge the SEP 1.x and SEP 2.0 networks and coexist on both networks. It is acknowledged
441 that, due to the unique position that an ALG will occupy in the HAN, security development
442 will be critical to minimize potential attack vectors.

443 • Security requirements for Over the Air upgradability

444 o Security requirements related to OTA are being addressed by the ZigBee Alliance as part of
445 the response to the CSWG review of the SEP 1.1 specification.

446 • Security requirements for Dual Mode Devices to ensure these do not become attack vectors

447 o All specification and security related development for Application Layer Gateways is being
448 referred to the ZigBee Alliance. Information has been added to the white paper clarifying
449 that the SEP 1.x and SEP 2.0 networks will not be bridged during the dual mode device
450 switching process and that a dual mode device, as envisioned by the White Paper, will only
451 operate on one network at a time.

452 • Requirements for testing security during upgrades and translations

453 o A specific section describing the anticipated HAN device migration process has been added
454 to the Appendix of the White Paper to clarify any misunderstanding by the CSWG on how
455 that process is intended to work. SEP 1.x and SEP 2.0 networks will not be bridged at any
456 point of the migration process.

457 • Clear communications with market participants/customers on security implementation, settings, and
458 maintenance during migration

459 o Specifications and security requirements for device migration is being referred to the ZigBee
460 Alliance for development. The Best Practices section in the White Paper is intended as a
461 guide to the ZigBee Alliance, Manufacturers and Utilities for the successful implementation
462 of a migration process.

463

SGAC REVIEW SECTION

ZigBee Response to the PAP 18 Response to the SGIP Smart Grid Architecture Committee review of the White Paper

The SGAC conducted a review of the PAP 18 white paper (version 1.0) and identified a number of concerns and issued a series of recommendations. The PAP 18 responses to these concerns and recommendations are below. The ZigBee Alliance response to the PAP 18 response is included here**:**

- Addressing the comments in Table 1 of this review

REF	Reference in White Paper	Comment	PAP18 Response	ZigBee Response
1	REQ.GW.1	SGAC has a concern about the feasibility of mapping SE 1 to SE 2 (Due to fundamental difference in the specifications and the application sets). Recommend the PAP add additional requirements such that the SSO develops appropriate mitigations.	PAP 18 will revise the paper to request the ZigBee Alliance highlight any issues found in the mapping of SE 1 to SE 2. The ZigBee Alliance will be responsible for developing a detailed mapping and how to handle missing functionality in either direction and establish rules for this mapping. Once this is developed the specific rules and functionality can be reviewed.	*The purpose of the PAP 18 white paper is to produce requirements and best practices for the stakeholders identified in the associated use cases, with the ZigBee Alliance as the main stakeholder. It is recognized that there are considerable differences in terms of protocol however SEP 1.x has been mapped to the CIM and SEP 2.0 is also based on the CIM. On that basis, there should be a reasonable mapping of functionality and the effort will be to ensure the functional mapping is represented correctly in the presentation and session protocol translation.*

2	REQ.GW.1	The inclusion of the gateway as a migration and coexistence option introduces additional security risk (Due to the security schemes terminating on either side). The product vendors will need to develop products that mitigate these concerns. Recommend the PAP add additional best practices language to instruct the SSO to carry through these recommendations to the manufacturers.	A specific note will be added to the ALG requirements for the ZigBee Alliance to detail the security implications and requirements in the ALG specification.	*The ZigBee Alliance agrees. The security issues and the mitigation strategy outlined in the specification document produced for the Application Layer Gateway (ALG) shall be clearly stated.*
3	REQ.GW.1	The SGAC request that the PAP clearly define ALG functionality in white paper.	PAP 18 believes it is more appropriate for the ZigBee Alliance to develop a more specific MRD and specification for the ALG based on the use cases identified. This will be added as a request to the ZigBee Alliance.	*Given the scope of the PAP 18 white paper, the ZigBee Alliance believes this should be covered in the specification document produced for the ALG.*

4	REQ.GW.1	The SGAC recognizes that, historically, ALGs have not been successfully deployed or maintained. While the SGAC is not advocating removal of these requirements, we would like additional language that notes the challenges. Recommend, the PAP add the concerns and require the SSO to develop appropriate mitigations.	PAP 18 notes in some cases ALG's have not been successfully deployed or maintained. However, ALGs have been very successful in the consumer electronics space. A reference to ALG maintenance will be added to the white paper and a need for continued maintenance as the Smart Energy Profiles are updated will be stressed to the ZigBee Alliance.	*PAP 18 addresses migration in many ways, including upgrading existing devices and development of new devices which will facilitate migration. The PAP 18 group was not asked to recommend a particular strategy; however the general aim is migration to a future standard, with the use of an ALG as a mitigation strategy for existing devices which cannot be upgraded. So whilst it is recognized that the architecture of an ALG is not ideal, the ALG is not proposed as a general product which will persist in the market place beyond a transition period as its sole purpose is as a mitigation strategy.*
5.	Generic	SGAC recommends that PAP 18 separate migration issues based on two major classification of HAN device (Smart Meter and HAN device). The devices have completely different ownership, depreciation, upgrade and connectivity challenges.	The white paper currently tries to be explicit on requirements for Utility ESI (e.g. Smart Meter) versus HAN devices because it is recognized their migration issues are different. A paragraph specifically addressing Utility ESI migration will be added to the Appendix of the white paper.	*The ZigBee Alliance agrees and recommends that PAP 18 distinguish these classes of devices.*

6.	Generic	The best practice recommendations may have significant cost implications (e.g., support both technologies). Recommend some disclaimer language that defers the decision or indicates that there are other drivers beyond the functionality (i.e., these are deployment decision that need to be weighed by the regulators, utilities and other stakeholders).	A note will be added to Migration Risks and Costs on this.	*The ZigBee Alliance has no particular statement on this comment as it is relevant to other stakeholders.*
7.	Generic	Paper is vague on the reason for migration. Why would customer migrate from one technology to the other? Are there known triggers? Does the service provider or the customer decided on the migration? Recommend that the PAP add some clarifying language.	There was not agreement in PAP 18 on reasons and trigger for migration from SE 1 to SE 2. As such it was left out of the white paper as it is believed this is a local decision and not something the PAP should decide.	*The ZigBee Alliance has no particular statement on this comment as it is relevant to other stakeholders.*
8.	Generic	Recommend the use case sections be labeled as informative (versus normative).	The use cases are all intended to be informative, only the requirements are normative.	*The ZigBee Alliance agrees that the section should be labeled as informative.*

9.		There are a number of recommendations in the document. It is not clear which option is preferred when compared to another option (e.g., all things being equal it is better to upgrade vs. coexist). Along these lines there is no impact assessment or feasibility assessment. As a general comment it would be helpful to add this analysis. If not possible due to the aggressive timeline, recommend the ZigBee Alliance be required to respond with impact and feasibility.	There was not agreement in PAP 18 on the preferred approach and it is believed this should be a local decision.	*The ZigBee Alliance has no particular statement on this comment however it does recognize that the PAP 18 group was not asked to recommend a particular strategy.*
10.	Generic	It is not clear in the paper which specification shoulders the mapping burden? Is the mapping maintained at a higher level and both specs are updated periodically to maintain consistency? Recommend the PAP add some additional requirements along these lines.	The mapping is a separate specification that would need to be updated with any update to SE 1 or SE 2. This will be noted for the ZigBee Alliance.	*The PAP 18 white paper provides requirements and recommendations to stakeholders. It should identify the main stakeholder (i.e. the ZigBee Alliance) however it should not make statements regarding mapping, rather identify requirements for managing mapping to the ZigBee Alliance.*

11.	REQ.ZA.1	The SGAC requests additional clarification on requirement REQ.ZA.1. The intended audience is not well defined (e.g., is this a requirement for the SSO?)	PAP 18 expected market participants would need to discuss and review which is why it was noted as the ZigBee Alliance as well as OpenSG. We will note that the ZigBee Alliance will propose the solution for ZA.1. The reference to OpenSG has been removed from the requirement.	*The ZigBee Alliance agrees that REQ.ZA.1 should be clearer regarding the intended stakeholders.*
12.	Generic	The SGAC noted, that certain flexibilities be constrained by time. For example, the best practices section states that the customer should have the flexibility to upgrade the device at the time of their choosing. It is unreasonable to assume that the service provider will be able to support competing versions of a technology indefinitely.	This comment will be added to the Best Practices section to note that Utilities and Service Providers may establish an end date beyond which migration is required or older devices are no longer supported in the HAN if they deem it appropriate.	*The ZigBee Alliance agrees that REQ.ZA.1 should be clearer regarding the intended stakeholders.*

13.	Generic	SGAC would like the document to include a statement about future green field deployments where both specifications are readily available. We would like the document recommend SEP2 because of the superior interoperability, functionality and security; subject to specification and product availability. SEP2 from the SGAC's perspective is a superior technology and better aligned with the SGIP requirements.	The PAP 18 scope was detailing the migration issues and best practices for migration from SE 1 to SE 2. The SGAC can recommend green field deployments use SE 2 when it is readily available but this was considered outside the scope of PAP 18.	*The ZigBee Alliance has no particular statement on this comment however it does recognize that the PAP 18 group was not asked to recommend a particular strategy. On the basis that it is a migration document, the assumption is that the aim is to migrate from SEP 1.x to SEP 2.0.*

*The full SGAC review and PAP 18 response to the SGAC review can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SEPTransitionAndCoexistenceWP, SGAC review, version 0.3 clean.

CSWG Appendix

The following table contains the detailed breakdown of suggestions for cyber security requirements that pertain to the NISTIR (Table 1) for the *"SEP 1.x to SEP 2.0 Transition and Coexistence White Paper"*.

Reference in Standard	Applicable NISTIR Requirement	CSWG Suggested Cybersecurity Requirement
REQ.ZA.3 A procedure shall be defined for replacing SEP 1.x security credentials with SEP 2.0 security credentials on a deployed device.	SG.AC-3: Account Management	The procedure shall ensure that the same access control policies are in effect from SEP 1.x to SEP 2.0.
	SG.AU-2: Auditable Events	All events in the credential replacement procedure shall be timestamped and included in an audit log.
	SG.CA-5: Security Authorization to Operate	The procedure shall include the security authority to operate when transitioning to SEP 2.0.

	SG.CM-3: Configuration Change Control	The procedure shall ensure the secure delivery of the SEP 2.0 security credentials.
	SG.IA-3: Authenticator Management	The procedure shall manage the authentication credentials and processes, including not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.
	SG.IA-4: User Identification and Authentication	The procedure shall ensure that users have the same identification and authentication requirements after the transition from SEP 1.x to SEP 2.0.
	SG.IA-5: Device Identification and Authentication	The procedure shall ensure that devices have the same identification and authentication requirements after the transition from SEP 1.x to SEP 2.0.
	SG.SC-11: Cryptographic Key Establishment and Management	The procedure shall ensure that the cryptographic key establishment and management is validated and tested after the replacement of the security credentials.
	SG.SC-14: Transmission of Security Parameters	The procedure shall ensure that the security credentials are reliably associated with correct data elements.
	SG.SC-26: Confidentiality of Information at Rest	The procedure shall ensure that the confidentiality of the information at rest in the device is not compromised during the security credential replacement.
	SG.SI-6: Security Functionality Verification	The procedure shall ensure the security function is verified after the credential replacement.
REQ.ZA.4 SEP 1.x HAN devices shall have the ability to perform a firmware migration (e.g., OTA, manual, etc.)	SG.AC-4: Access Enforcement	The migration process shall ensure that access rules are strictly enforced during the firmware migration.
	SG.AU-2: Auditable Events	All significant events taking place during the migration shall be timestamped and included in an audit log.
	SG.CM-5: Access Restrictions for Configuration Change	The migration process shall ensure that only authorized entities may perform the migration.
	SG.CM-6: Configuration Settings	The migration process shall ensure that security-related configuration settings are maintained.
	SG.CM-7: Configuration for Least Functionality	The migration process shall ensure that the principle of “least functionality” shall be maintained.
	SG.CM-11: Configuration Management Plan	The migration process shall include a configuration management plan.

	SG.IA-5: Device Identification and Authentication	The procedure shall ensure that devices have the same or improved identification and authentication requirements after the migration from SEP 1.x to SEP 2.0.
	SG.MA-3: Smart Grid Information System Maintenance	The migration process shall ensure that any changes to maintenance procedures required by SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the migration planning.
	SG.MA-6: Remote Maintenance	The migration process shall ensure that any changes to maintenance procedures required by SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the migration planning.
	SG.MA-7: Timely Maintenance	The migration process shall ensure that any changes to maintenance procedures required by SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the migration planning.
	SG.SC-26: Confidentiality of Information at Rest	The procedure shall ensure that the confidentiality of the information at rest in the device, including its security credentials, is not compromised during the migration.
	SG.SI-6: Security Functionality Verification	After the migration process, security functionality shall be verified.
3.1.2 ALG Specific Requirements … An ALG enabling translation between SEP 1.x and SEP 2.0 must be able to maintain the security of HAN devices communicating with the ALG. It is expected that each application (e.g., SEP 1.x) is secure and that the ALG is reasonably fortified against attack. Security can be maintained by pairs of devices, hop-to-hop, along a communications path when intermediaries can be trusted.	SG.AC-1: Access Control Policy and Procedures	An Access Control policy shall be developed for the ALG.
	SG.AC-3: Account Management	The ALG shall ensure that the appropriate access control policies are in effect during translations between SEP 1.x and SEP 2.0.
	SG.AU-2: Security Awareness	All significant events taking place during the migration shall be timestamped and included in an audit log.
	SG.CA-5: Security Authorization to Operate	The ALG shall include the security authority to operate when translating between SEP 1.x and SEP 2.0.
	SG.CM-3: Configuration Change Control	The ALG shall ensure that all SEP 1.x security requirements continue to be met or improved.
	SG.IA-3: Authenticator Management	The ALG shall manage the authentication credentials and processes for both SEP 1.x and SEP 2.0, including not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.

	SG.IA-4: User Identification and Authentication	The ALG shall ensure that users have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.IA-5: Device Identification and Authentication	The ALG shall ensure that devices have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.SC-10: Trusted Path	The trustworthiness of communications paths and intermediaries shall be established before pairs of devices may assume they are to be trusted.
	SG.SC-11: Cryptographic Key Establishment and Management	The ALG shall handle key establishment and management for all SEP 1.x and SEP 2.0 devices with which it is communicating.
	SG.SC-26: Confidentiality of Information at Rest	The ALG shall ensure that the confidentiality of the information at rest, including its security credentials, is not compromised during translations.
REQ.GW.2 When the Utility ESI (e.g. Smart Meter) SEP firmware is migrated to SEP 2.0, an ALG equipped to translate between SEP 2.0 and SEP 1.x networks shall enable existing SEP 1.x devices to continue to be active and function.	SG.AC-1: Access Control Policy and Procedures	An Access Control policy shall be developed for the ALG.
	SG.AC-3: Account Management	The ALG shall ensure that the appropriate access control policies remain in effect for SEP 1.x devices.
	SG.AU-2: Auditable Events	All significant events taking place during the migration shall be timestamped and included in an audit log.
	SG.CA-5: Security Authorization to Operate	The ALG shall include the security authority to operate when translating between SEP 2.0 and SEP 1.x.
	SG.CM-3: Configuration Change Control	The ALG shall ensure that all SEP 1.x security requirements continue to be met or improved.
	SG.IA-4: User Identification and Authentication	The ALG shall ensure that users have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.IA-5: Device Identification and Authentication	The ALG shall ensure that devices have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.SC-26: Confidentiality of Information at Rest	The ALG shall ensure that the confidentiality of the information at rest is not compromised in SEP 1.x devices, including their security credentials.
REQ.DM.1 Dual Mode devices shall be capable (e.g. automatically, manually, etc.) of switching from one SEP	SG.AU-2: Auditable Events	All significant events taking place during the switching shall be timestamped and included in an audit log.

firmware to another. REQ.DM.3 For deployed Dual Mode devices, a method shall be available to verify the SEP 2.0 firmware versions and update if necessary prior to a SEP 1.x to SEP 2.0 migration.	SG.AC-3: Account Management	The dual mode switching capability shall ensure that the same access control policies are in effect from SEP 1.x to SEP 2.0.
	SG.CM-5: Access Restrictions for Configuration Change	The dual mode switching capability shall ensure that only authorized entities may perform the switching.
	SG.CM-6: Configuration Settings	The dual mode switching capability shall ensure that security-related configuration settings are maintained.
	SG.CM-7: Configuration for Least Functionality	The dual mode switching capability shall ensure that the principle of "least functionality" shall be maintained.
	SG.CM-11: Configuration Management Plan	The dual mode switching capability shall follow a configuration management plan.
	SG.IA-5: Device Identification and Authentication	The dual mode switching capability shall ensure that devices have the same or improved identification and authentication requirements after the switching between SEP firmware applications.
	SG.MA-3: Smart Grid Information System Maintenance	The dual mode switching capability shall ensure that any changes to maintenance procedures required by SEP 1.x and SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the switching planning.
	SG.MA-6: Remote Maintenance	The dual mode switching capability shall ensure that any changes to maintenance procedures required by SEP 1.x and SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the switching planning.
	SG.MA-7: Timely Maintenance	The dual mode switching capability shall ensure that any changes to maintenance procedures required by SEP 1.x and SEP 2.0, including remote maintenance and changes in timing of maintenance are included as part of the switching planning.
	SG.SC-26: Confidentiality of Information at Rest	The dual mode switching capability shall ensure that the confidentiality of the information at rest in the device, including its security credentials, is not compromised during the switching.
	SG.SI-6: Security Functionality Verification	After dual mode switching, the security functionality shall be verified.

REQ.SEP.5 The requirements for obtaining SEP 2.0 security credentials and replacing SEP 1.x security credentials with SEP 2.0 security credentials shall be communicated to market participants, if supported.	SG.PM-1: Security Policy and Procedures	Security policies and procedures shall be made available to market participants.
REQ.SEP.6 SEP 2.0 security credentials for each HAN device in the field shall be available, assigned and downloaded to a unique HAN device based on its MAC address.	SG.AU-2: Auditable Events	All significant events taking place during the download process shall be timestamped and included in an audit log.
	SG.IA-3: Authenticator Management	The procedure shall manage the authentication credentials and processes, including not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.
	SG.IA-5: Device Identification and Authentication	The security credential process shall ensure that HAN devices have the same identification and authentication requirements during the download process.
	SG.SI-6: Security Functionality Verification	After the download of the security credentials, the security functionality shall be verified.
REQ.SEP.7 Manufacturers shall ensure that their HAN devices implement the procedure for replacing SEP 1.x security credentials with SEP 2.0 security credentials on deployed devices.	SG.AC-3: Account Management	The manufacturer's procedure shall ensure that the same access control policies are in effect from SEP 1.x to SEP 2.0.
	SG.AU-2: Auditable Events	All events in the credential replacement manufacturer's procedure shall be timestamped and included in an audit log.
	SG.CA-5: Security Authorization to Operate	The manufacturer's procedure shall include the security authority to operate when transitioning to SEP 2.0.
	SG.CM-3: Configuration Change Control	The manufacturer's procedure shall ensure the secure delivery of the SEP 2.0 security credentials.
	SG.IA-3: Authenticator Management	The manufacturer's procedure shall manage the authentication credentials and processes, including not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.
	SG.IA-4: User Identification and Authentication	The manufacturer's procedure shall ensure that users have the same identification and authentication requirements after the transition from SEP 1.x to SEP 2.0.

	SG.IA-5: Device Identification and Authentication	The manufacturer's procedure shall ensure that devices have the same identification and authentication requirements after the transition from SEP 1.x to SEP 2.0.
	SG.SC-11: Cryptographic Key Establishment and Management	The manufacturer's procedure shall ensure that the cryptographic key establishment and management is validated and tested after the replacement of the security credentials.
	SG.SC-14: Transmission of Security Parameters	The manufacturer's procedure shall ensure that the security credentials are reliably associated with correct data elements.
	SG.SC-26: Confidentiality of Information at Rest	The manufacturer's procedure shall ensure that the confidentiality of the information at rest in the device is not compromised during the security credential replacement.
	SG.SI-6: Security Functionality Verification	The manufacturer's procedure shall ensure the security function is verified after the credential replacement.
REQ.SEP.8 Where applicable, the over the air (OTA) upgrade process for HAN Devices to migrate from SEP 1.x to SEP 2.0 shall be clearly defined and communicated.	SG.PM-1: Security Policy and Procedures	Security policies and procedures shall be clearly defined and communicated to all stakeholders.
REQ.SEP.9 Utilities shall communicate how to Register HAN devices to the Utility ESI based on what SEP firmware is in the Utility ESI (e.g., Smart Meter).	SG.PM-1: Security Policy and Procedures	Security policies and procedures shall be clearly defined and communicated to all stakeholders.
REQ.GW.8 An ALG providing translation between SEP 1.x and SEP 2.0 shall provide link layer, application layer and platform security in order to not degrade security for the HAN	SG.AC-1: Access Control Policy and Procedures	An Access Control policy shall be developed for the ALG.
	SG.AC-3: Account Management	The ALG shall ensure that the appropriate access control policies are in effect during translations between SEP 1.x and SEP 2.0.
	SG.AU-2: Security Awareness	All significant events taking place during the migration shall be timestamped and included in an audit log.
	SG.CA-5: Security Authorization to Operate	The ALG shall include the security authority to operate when translating between SEP 1.x and SEP 2.0.
	SG.CM-3: Configuration Change Control	The ALG shall ensure that all SEP 1.x security requirements continue to be met or improved.

	SG.IA-3: Authenticator Management	The ALG shall manage the authentication credentials and processes for both SEP 1.x and SEP 2.0, including not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.
	SG.IA-4: User Identification and Authentication	The ALG shall ensure that users have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.IA-5: Device Identification and Authentication	The ALG shall ensure that devices have the same identification and authentication requirements during translations between SEP 1.x and SEP 2.0.
	SG.SC-10: Trusted Path	The trustworthiness of communications paths and intermediaries shall be established before pairs of devices may assume they are to be trusted.
	SG.SC-11: Cryptographic Key Establishment and Management	The ALG shall handle key establishment and management for all SEP 1.x and SEP 2.0 devices with which it is communicating.
	SG.SC-26: Confidentiality of Information at Rest	The ALG shall ensure that the confidentiality of the information at rest, including its security credentials, is not compromised during translations.

Table of National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628 Security Requirements

The high-level security requirement families of the NISTIR 7628, *Guidelines for Smart Grid Cyber Security*[1], are shown in Table 2-1.

Table 2-1: NIST Smart Grid Security Requirements Families

NISTIR Ref.	NISTIR Smart Grid Security Requirement Families	Description
SG.AC	Access Control	The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified.
SG.AT	Security Awareness and Training	Implementing a Smart Grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities.
SG.AU	Audit and Accountability	Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating

[1] The three volumes of the NISTIR 7628 is available for download at http://csrc.nist.gov/publications/PubsNISTIRs.html

		correctly.
SG.CA	Security Assessment and Authorization	Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.
SG.CM	Configuration Management	The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration.
SG.CP	Continuity of Operations	Continuity of operations addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources.
SG.IA	Identification and Authentication	Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.
SG.ID	Information and Document Management	Information and document management is generally a part of the organization records retention and document management system.
SG.IR	Incident Response	Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the Smart Grid information system's operational status after the occurrence of a disruption.
SG.MA	Smart Grid system Development and Maintenance	Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.
SG.MP	Media Protection	The security requirements under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media.
SG.PE	Physical and Environmental Security	Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access Smart Grid information systems and components. Environmental security addresses the safety of assets from damage from environmental concerns. Physical and environmental security addresses protection from environmental threats.
SG.PL	Strategic Planning	The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to Smart Grid information system operation. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain Smart Grid information system operation during and after an interruption, and planning to identify mitigation strategies.
SG.PM	Security Program Management	The security program lays the groundwork for securing the organization's enterprise and Smart Grid information system assets. Security procedures define how an organization implements the security program.
SG.PS	Personnel Security	Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination.
SG.RA	Risk Management and Assessment	Risk management planning is a key aspect of ensuring that the processes and technical means of securing Smart Grid information systems have fully

		addressed the risks and vulnerabilities in the Smart Grid information system.
SG.SA	Smart Grid system and Services Acquisition	Smart Grid information systems and services acquisition covers the contracting and acquiring of system components, software, firmware, and services from employees, contactors, and third parties.
SG.SC	Smart Grid System and Communication Protection	Smart Grid information system and communication protection consists of steps taken to protect the Smart Grid information system and the communication links between Smart Grid information system components from cyber intrusions. Although Smart Grid information system and communication protection might include both physical and cyber protection, this section addresses only cyber protection.
SG.SI	Smart Grid System and Information Integrity	The security requirements described under the Smart Grid information system and information integrity family provide policy and procedure for identifying, reporting, and correcting Smart Grid information system flaws.

494
495
496
497
498
499
500

END DOCUMENT