Smart Energy Profile (SEP) 1.x Summary and Analysis

NATIONAL ELECTRIC SECTOR CYBER SECURITY ORGANIZATION RESOURCE (NESCOR)

Version 1.0

10/31/2011

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

The research was paid for by the Department of Energy (DOE) under the NESCOR grant.

Acknowledgments:

Project Manager – Annabelle Lee

Principle Investigators – Annabelle Lee and Glen Chason

The following individuals are members of this working group and have contributed their time, technical expertise, and commitment to developing this document:

William Foster, Sami Ayyorgun, Galen Rasche, Rob Alexander, Richard Kelsey, Slade Griffin, Stephen Chasko, Bill Cloutier, Tobin Richardson, Skip Ashton, Don Sturek, Robert Cragie, Himanshu Khurana, Andrew Wright, Marianne Swanson, Don Von Dollen, Erfan Ibrahim, Ido Dubrawsky, Scott Palmquist, David Kravitz, Tam Do, Vicky Pillitteri, Will Arensman, Larry Korhmann, Wendy Al-Mukdad, Alan Greenberg, Roger Levy, Charles McParland, Christopher Villarreal, Apurva Mohan, Justin Searle, Akhlesh Kaushiva, John Sucec, Alan Rivaldo, Anna Grau, Daniel Thanos, Vincent Bemmel, Quynh Dang, Zahra Makoui, Mark Ward, Raj Iyengar, Catherine Martinez, Mark Ellison, Dave Watson, Tom Herbst, Jan Krepelka, David Scott, Tom Markham, Kostas Tolios, and Justin Searle.

In particular, the following individuals developed major portions of this document and provided technical expertise: Skip Ashton, Don Sturek, Robert Cragie, John Sucec, Vicky Pillitteri, Will Arensman and his team, Apurva Mohan, Himanshu Khurana, and Tom Markham.

We would also like to offer special thanks to the ZigBee Alliance that provided this working group with copies of all the documents that we requested.

Executive Summary

Load control capabilities in Home Area Networks (HANs) are an integral part of the smart grid and energy efficiency modernization efforts currently underway. Like other smart grid systems, HANs are vulnerable to cyber attacks and adequate security measures are needed. The Zigbee Smart Energy Profile 1.0 and Smart Energy Profile 1.1 (collectively referred to in this white paper as SEP 1.x) present a communication framework for HAN devices along with a security framework.

This white paper builds upon prior efforts that assessed the security of SEP 1.x with a primary objective to help stakeholders understand the vulnerabilities in SEP 1.x and provide them with actionable advice on how to mitigate or minimize these vulnerabilities. This white paper goes beyond prior work in several aspects. Included are several representative system architectures and the Texas public utilities commission architecture. These representative architectures assist in understanding the results of the security analysis. This white paper lists the differences between versions SEP 1.0 and 1.1 of the specifications, which will help the relevant stakeholders to understand the applicability of this document on their HANs. Finally, this document presents potential vulnerabilities, impacts, best practices, and mitigations for SEP 1.x.

Sections 1 through 4 include a summary of SEP 1.x including the security functionality, security controls, and cryptographic primitives. Section 5 includes a mapping of the security requirements to the National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* requirements. Section 6 includes best practices and identifies vulnerabilities, and mitigation strategies for the vulnerabilities. To implement the security and mitigation policies presented in Section 6, a secure and robust Trust Center is needed that will ensure that vulnerabilities in the SEP 1.x can be mitigated. Section 6 also demarcates the boundary and scope of the security analysis in this white paper and identifies some implementation issues that need to be addressed.

Table of Contents

List of Figures

List of Tables

1 Background

The National Electric Sector Cybersecurity Organization Resource (NESCOR) technical working group (TWG) 1 has created a sub-group to specifically address the first two versions of the ZigBee Smart Energy Profiles (SEP) - SEP 1.0 and 1.1. These are referred to as SEP 1.x in this document. To assist utilities, regulators, and integrators who are deploying and configuring SEP 1.x in field devices, NESCOR, the Cyber Security Working Group (CSWG), and other experts have developed this technical white paper to provide guidance on the use of both profiles.

1.1 Scope

This white paper includes an overview of the SEP 1.x specification and identifies security gaps, potential vulnerabilities, impacts and mitigation strategies and builds upon security reviews done in the past such as the CSWG review, Carnegie Mellon University (CMU) review, and other independent reviews. The difference between the two versions of the SEP specifications was assessed to consider the impact of these security gaps on each one of them. Security requirements were also identified from the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* document. Finally, recommendations are made on how the SEP 1.x profile should be used in deployments.

The approach taken in this white paper is to identify the security gaps and potential vulnerabilities and assess their impact on the Home Area Networks (HANs) that are deployed using the SEP 1.x. The impact is analyzed using a risk management approach where the security threats are considered based on the risks they pose to the HAN. This white paper identifies compensating controls and best practices to mitigate or minimize the identified risks, where applicable. Ideally, these compensating controls and best practices will be specified in such a way that they are compliant with SEP 1.x and can be implemented in deployed or to-be-deployed SEP 1.x based HANs. This white paper identifies risks that cannot be entirely mitigated so that the entities deploying ZigBee HANs understand them and account for them in their deployments.

This white paper is focused on the SEP 1.x specification used in HAN deployments. There are several other network architectures connected to the HAN, such as a Neighborhood Area Network (NAN), backhaul network, and other non-ZigBee interfaces within a HAN. This white paper does not assess these networks because they either do not use ZigBee technology or their architectures and security are not sufficiently detailed in the SEP 1.x specification. This white paper also identifies areas like NAN security as a network impacting HAN security and recommends the applicable

standards bodies consider their architectures and security in detail in future versions of the specifications.

2 Representative System Architectures

Smart energy networks primarily have two types of devices - a smart meter which bridges a HAN to a NAN and ZigBee home devices that are part of a single HAN. Smart meters and HAN devices use ZigBee to communicate across the network. The SEP 1.x specification allows for different network topologies. One topology is where ZigBee devices join a smart energy network coordinated by a smart meter. In this topology, a smart meter coordinates network management and security. In a second topology, the ZigBee devices do not join a smart energy network but create a home area network for the consumer called a Consumer Private – Home Area Network (CP-HAN). In a CP-HAN a device creates an application level bridge between the smart energy network and the CP-HAN. This device is called an Application Layer Gateway (ALG) and is the ZigBee network coordinator for the CP-HAN. Networks with smart meters acting as the coordinator are called Utility Enabled – Home Area Networks (UE-HAN). In another topology, the ALG is the ZigBee network coordinator and Trust Center for the CP-HAN. In this third topology there is no UE-HAN and the smart meter provides the usage data (and optionally the public pricing data) to the ALG acting as an information sensor.

Figure 1 illustrates a sample architecture that shows an interconnection between a smart meter and a field area network, the Advanced Metering Infrastructure (AMI). For this white paper, the AMI interface and the field area network are out of scope.

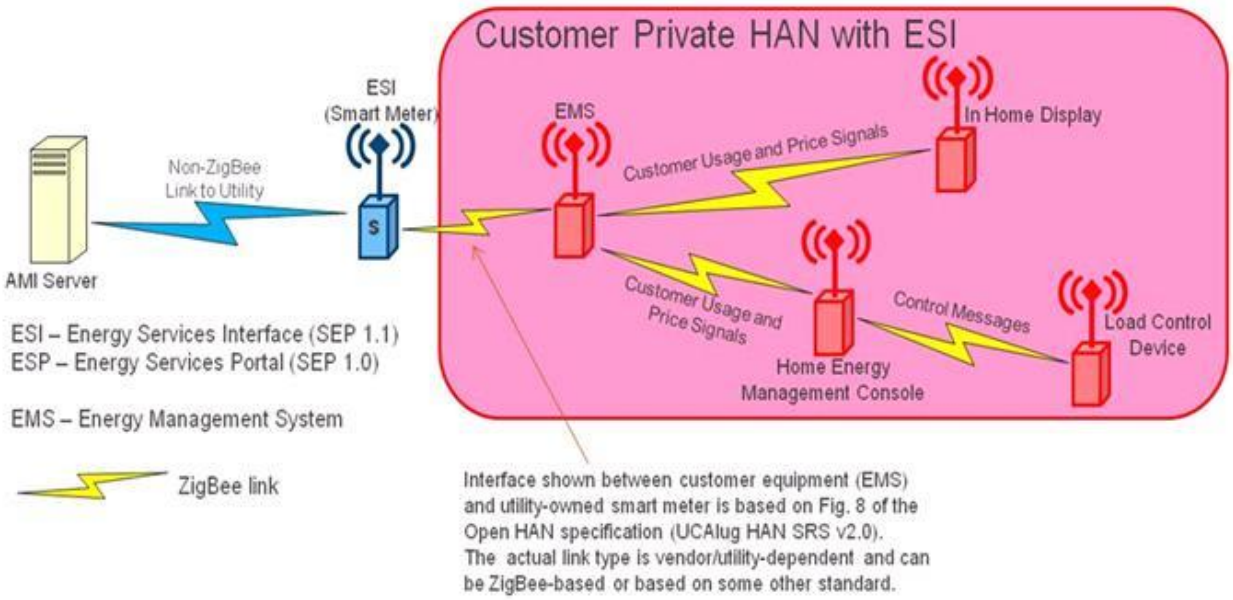

Figure 1 – CP-HAN with ESI[1]

Figures 2, 3, and 4 below delineate the scope of this summary and analysis. Figure 2 depicts a UE-HAN and its connection, through a utility meter, to a utility backend environment. The utility meter, along with its ZigBee radio interface, serves as the ZigBee Media Access Control layer coordinator, as the SEP 1.x Trust Center, and as the utility HAN's Energy Services Interface (ESI). The utility meter and all the ZigBee devices attached to the UE-HAN are within the scope of this white paper and their functionality are relevant to the security analysis found in this document. Security issues of the AMI domain in the smart meter and upstream of the physical utility meter and throughout the utility backend environment are outside the scope of this white paper. Within the UE-HAN, security aspects of those portions of home appliances and displays not directly involved in ZigBee communications and control functions are outside the scope of this white paper.

Figures 3 and 4 depict UE-HANs that contain gateway nodes that allow nodes on the UE-HAN to communicate with those located on residential networks. Descriptions and implementation details of these networks are unknown at this time; therefore, their security environment and any analysis of security-related issues are outside the scope of this white paper. Since the primary function of these inter-HAN gateways is to

[1] J. Sucec, S. Ayyorgun under NESCOR contract

promote communications with nodes within the UE-HAN, these gateways have security-related issues. While the UE-HAN portion of a design may appear adequately secure, the full impact on the security of a UE-HAN can only be determined through analysis of all the connected devices, application level software, and communications protocols

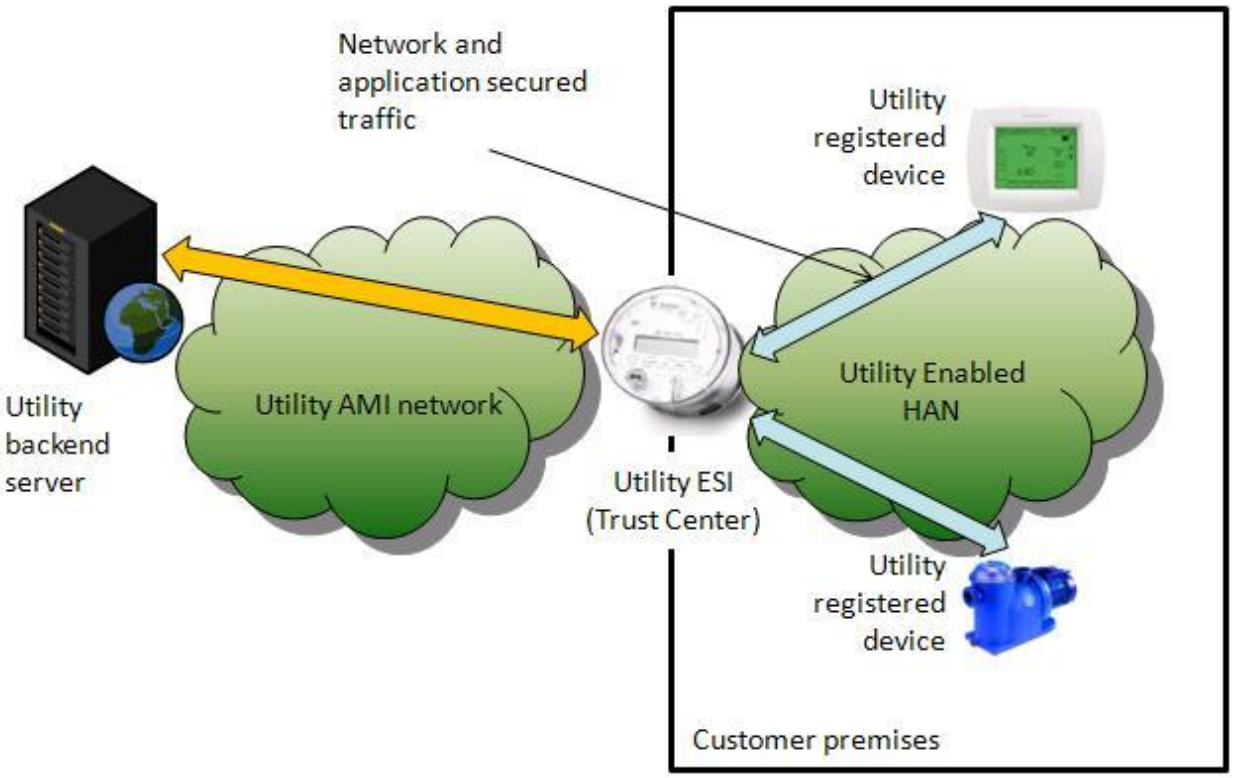

Figure 2 – Utility Enabled HAN (UE-HAN)

In Figure 2, all devices in the premises are managed by the utility and have to be registered with the Utility. There is one HAN, the Utility Enabled HAN (UE-HAN), in the premises.

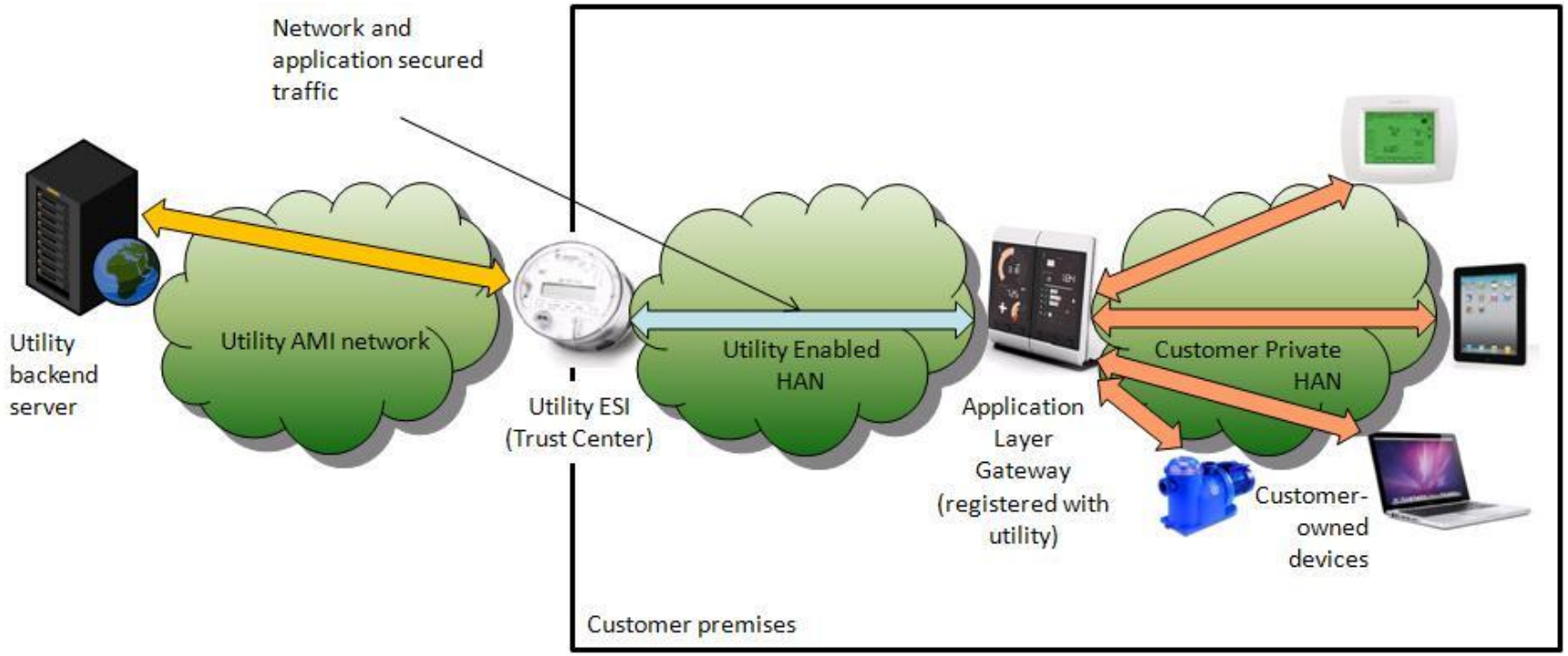

Figure 3 - Consumer Private HAN (CP-HAN)

In Figure 3, there is one device that has to be registered with the Utility. It is shown as an ALG in the figure. This device must be a SEP 1.x compliant device. There are two separate HANs in the premises, a UE-HAN and a CP-HAN, each with its own Trust Center. The devices on the CP-HAN do not have to be registered with the Utility and their functionality is independent of the SEP 1.x specification. The coupling between the UE-HAN and the CP-HAN depends on the

functionality of the ALG. This white paper only addresses the UE-HAN and the devices registered with the utility (ALG in this figure). The CP-HAN and the customer-owned devices on the CP-HAN are outside the scope of this white paper.

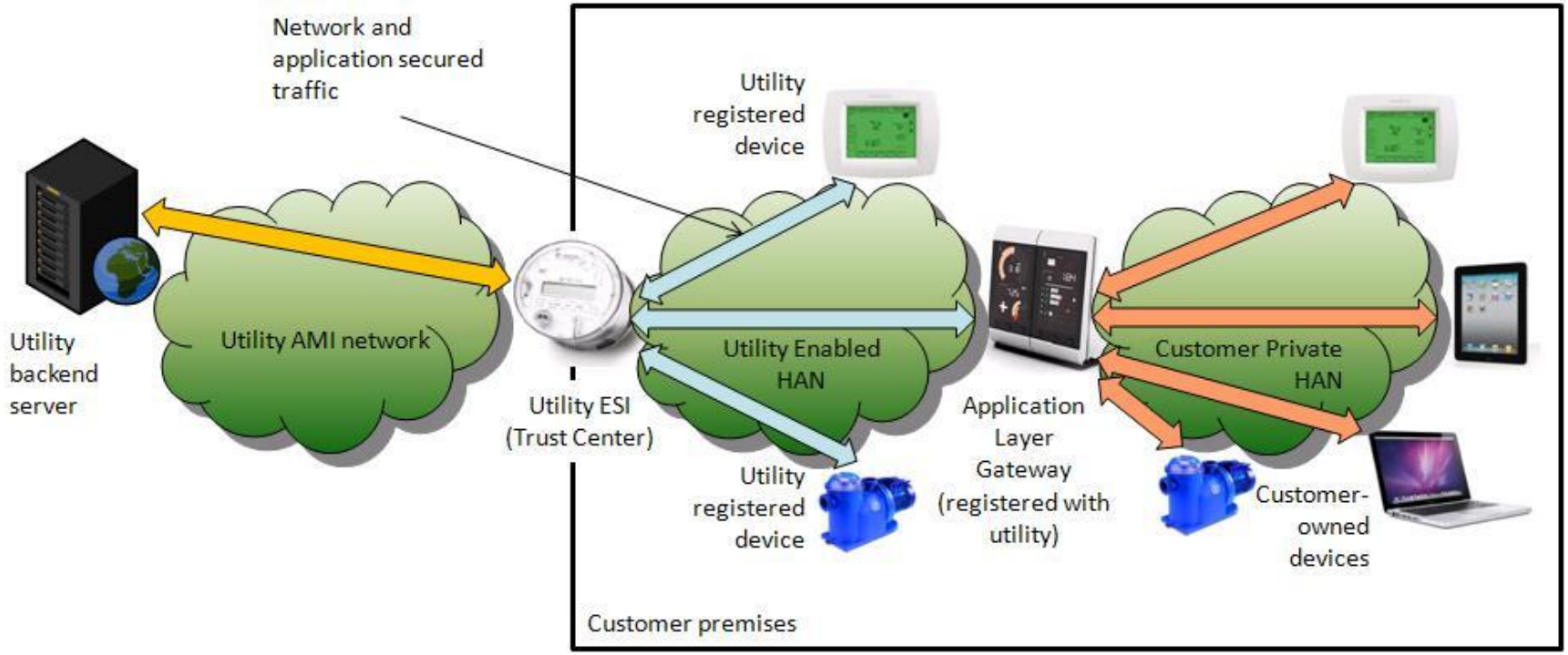

Figure 4 - Utility Enabled and Consumer Private HANs (UE-HAN and CP-HAN)

In Figure 4, some devices in the premises are solely managed by the utility and have to be registered with the Utility. An additional ALG is owned by the customer but must be a SEP 1.x compliant device and must be registered with the Utility.

There are two separate HANs in the premises; a UE-HAN and a CP-HAN, each with its own Trust Center. The devices on the CP-HAN do not have to be registered with the Utility and their functionality is independent of the SEP 1.x specification. The coupling between the UE-HAN and the CP-HAN depends on the functionality of the ALG. This white paper only addresses the UE-HAN and the devices registered with the utility. The CP-HAN and the customer-owned devices on the CP-HAN are outside the scope of this white paper.

2.1 Texas Implementation

A high-level view of the parties that interact in the competitive market within the Electric Reliability Council of Texas (ERCOT) region of Texas is included in Figure 5. The UE-HAN is provisioned and de-provisioned through the Smart Meter Texas (SMT) portal. There are currently four Transmission/Distribution Service Providers (TDSPs) who participate in SMT: AEP Texas, CenterPoint, Oncor, and Texas New Mexico Power. In addition to these TDSPs, retail electric providers, third-party providers, manufacturers of HAN devices and intelligent appliances, and consumers may all interact with the SMT portal.

The SMT program allows the consumer (residential and business customers) to become active participants in practicing energy efficiency in the home or business. The SMT program allows the consumer to:

- View and analyze energy usage data in 15 minute increments and use the data to understand energy usage patterns; possibly reducing electricity usage and costs,
- Setup a CP-HAN and smart appliances, such as a thermostat, refrigerator, or other smart devices, and
- Raise awareness of waste and the carbon footprint.

In this architecture, the communications to the UE-HAN can use the Internet through a home gateway or the meter backhaul network. The internet connection and the meter backhaul network are not specified by ZigBee and are outside the scope of this white paper.

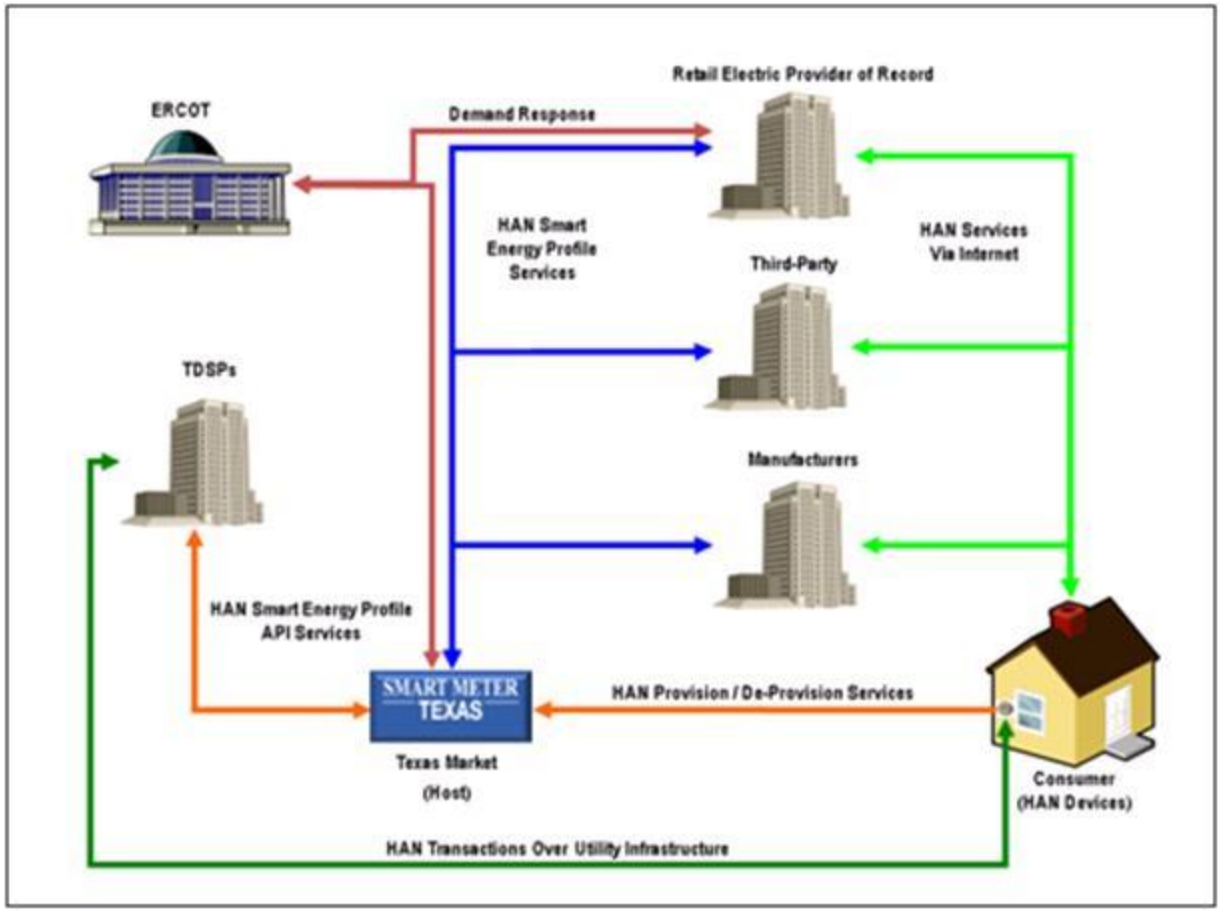

Figure 5 - Texas Smart Grid Actors and Communication Paths

A draft illustration of the communications pathway implemented in the ERCOT market in Texas that enables the registration of HAN devices in the UE-HAN is included in Figure 6.

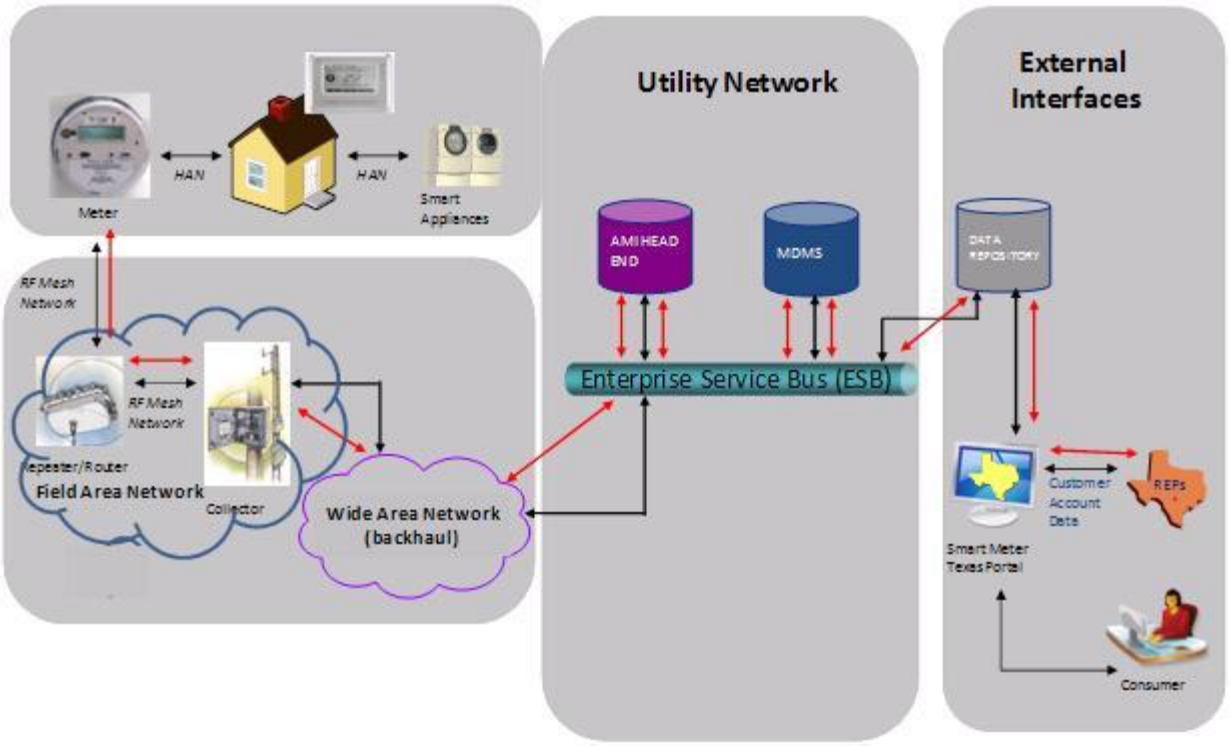

Figure 6 – Texas HAN Communications Path and Interface

(Note: There are many other communications networks in this diagram. Only the UE-HAN network in the upper left is in scope for SEP 1.x and this white paper.)

2.2 California

The California Public Utility Commission (CPUC) posted Decision 11-07-056 that is effective on July 28, 2011. The decision requires the three California Independent Operating Units (IOUs), Pacific Gas and Electric (PG&E), San Diego Gas and Electric (SDG&E), and Southern California Edison (SCE) to develop Smart Meter HAN implementation plans specific to each. Following are the major requirements for the implementation plans.

- Each implementation plan should include an estimated rollout implementation strategy, including a timetable, for making HAN functionality and benefits generally accessible to customers in a manner similar across all three IOUs.
- The implementation plans should include an initial phase with a rollout of up to 5,000 HAN devices, which would allow for HAN activation for early adopters

upon request, even if full functionality and rollout to all customers awaits resolution of technology and standards issues.

- The implementation strategy for HAN activation should discuss key issues, such as:
    - Costs,
    - Expanded data access and data granularity,
    - Current and evolving national standards and security risk mitigation and best practices,
    - Responsibilities for secure HAN connection,
    - Outcomes from working on HAN device interoperability,
    - Security testing and certification methodologies developed in collaboration with interested third parties (e.g., Lawrence Berkeley National Laboratories or California State University-Sacramento),
    - Customer needs and preferences,
    - A strategy for learning from the initial rollout, and
    - Provisions for accommodating customers' efforts to utilize HAN functionality independent of the utility.
- Finally, the full rollout shall require smart meters to transmit energy usage data to the home so that a HAN device of the consumer's choice can receive it.

3 SEP 1.0 and SEP 1.1 Differences

The main changes between SEP 1.0 and SEP 1.1 are the addition of Trust Center swapout/replacement recommendations (which is not applicable to normal usage), clarification on the installation code, and the addition of the over the air (OTA) upgrade cluster. Following is a more detailed description of the revisions from SEP 1.0 to SEP 1.1:

1. Moved text regarding registration, re-registration, de-registration to make it normative.

2. Added text regarding Trust Center swapout/replacement procedures. This is fundamentally about how keys are stored and backed up and transferred. (Note: This is not final and is subject to change.)
3. More prescriptive about post-joining procedure regarding service discovery.
4. Added text allowing the Trust Center to add and remove device keys.
5. Added text to explicitly discover the Key Establishment Cluster.
6. Clarified Trust Center brokering of link keys.
7. Clarified on installation code format.
8. Added formal procedure for device joining, service discovery, and device binding to tighten up interoperability.
9. Added OTA upgrade.
10. Added multiple ESI guidelines.
11. Added tunneling cluster.
12. Tighter definition of Smart Energy device and the concept of logical devices.
13. Many changes to metering cluster.
14. Added mirroring to metering cluster.
15. Many changes to price cluster.
16. Annex B.7 is added – best practices for Inter-PAN Transmission.
17. Added prepayment cluster (Note: As stated in the specification, “The Prepayment Cluster description in this revision of this specification is provisionary and not certifiable. This feature set may change before reaching certifiable status in a future revision of this specification.” See Annex D.7 of [2]).

This white paper focuses on items 1 – 9 listed above and the security relevance of the changes.

3.1 SEP 1.1 other changes

1. The term ESP has been replaced by ESI.

2. The term 'unsecured rejoin' is deprecated.
3. OTA bootload cluster was specified in a separate document (ZigBee document 095264r15).

4 ZigBee SEP 1.x Overview

Included in this section is an overview of the security functionality specified for the ZigBee SEP 1.x. The specification provides standard interfaces and device definitions to allow interoperability among ZigBee devices produced by various manufacturers of electrical equipment, meters, and Smart Energy enabling products.[2]

The ZigBee PRO stack specification [27] defines two modes of security operation primarily defined around the key types used. The two modes are standard and high. High security mode is not specified in SEP 1.x and is not discussed further in this white paper.

4.1 SEP 1.1 Keys

One of the major components of SEP 1.x is cryptography used for authentication, integrity, and confidentiality. Table 1 provides references for the cryptographic keys used in SEP 1.x.

Table 1 - Details of cryptographic keys

Key name	Key Shared with	Related protocol stack layer	Key establishment or updated references
Pre-configured link key	Trust center	Application layer	[2] Section 5.4.8.1, [2] Annex F.
Trust center link key	Trust center	Application layer	[2] Section 5.4.7.
Network key	Entire HAN	Network layer	[2] Section 5.4.2, [2] Section 5.4.4.
Link key	Pair-wise device	Application layer	[2] Section 5.4.7.4.

[2] The purpose was extracted from the SEP 1.x document [2].

4.2 Trust Center

To function securely in a network, a device must have a counterpart device from which it can obtain trusted keys and control access. This role is performed by the Trust Center, which is required in any ZigBee Smart Energy network. The Trust Center performs the following functions:

1. Generates the network key to be used in the network
2. Configures a device with its key(s)
3. Controls access to the network
4. Acts as a trust broker to help devices establish pair-wise link keys
5. Implements the network management policies
6. Implements the network security policies
7. Stores keys for the network

The role of the Trust Center is defined in the SEP 1.x specification, but only the operation of the device serving as the Trust Center is defined. This includes functions 1 through 4 above. The SEP 1.x specification requires the Trust Center to implement and enforce the policies listed in functions 5 and 6 above, but does not provide specific guidelines on how this is to be done.

SEP 1.x references memory and device protection, physical protection/tamper evidence, and secure storage. These are described as functions of the meter and are outside the scope of the SEP 1.x specification and this white paper.

Guidelines for Trust Center behavior such as basic operation, key updates and other Trust Center recommendations are covered in ZigBee document 08-5195-02 (ZigBee PRO Trust Center Best Practices) [3] and the ZigBee specifications [1][2]. The Trust Center Best Practices document defines policies and roles for the Trust Center but these are specified as best practices and are not requirements. They are referenced in this analysis as best practices, but are not assessed because they are not requirements. For example, the best practices document notes that it is important for the Trust Center to periodically distribute a new network key but no requirements on how often this should occur are specified. The best practices document identifies factors to be considered on the periodicity of network key updates such as devices joining or

leaving the network, but it is up to individual deployments to specify a frequency of update.

4.3 SEP 1.x Network

The following section provides an overview of a SEP 1.x network.

Network Coordinator: When a ZigBee device is initially powered up, it can either join a network or create a network. If creating a network, the device serves as the *network coordinator*. For example, in the case of a UE-HAN, the meter serves as the network coordinator and the Trust Center. When initially powered up, the network coordinator establishes the network and its configuration. To advertise its availability the network coordinator responds to device beacon requests by sending a beacon message containing the network configuration.

Figure 7 – Device Joining

Device Joining Unauthenticated: If not serving as network coordinator, a ZigBee device starts searching for a network beacon from a network coordinator when the device is powered on. If the device finds a beacon it reads the beacon and joins the network as an unauthenticated device, see Figure 7 above. This establishes an association between the Trust Center and the device.

Device Joining Authenticated: Before being allowed to join a network as an authenticated device, the device's identity must first be established with the Trust Center. The Install Code is defined within the SEP 1.x specification to provide device and network pairing. When ZigBee compliant devices are manufactured, the manufacturer selects an installation code that can be 48, 64, 96 or 128 bits long. This installation code is printed on the device (see section 5.4.8.1 of [2]). The user utilizes an out-of-band mechanism that is outside the scope of the SEP 1.x specification, to convey the device unique installation code to the utility. The installation code may be provided by the homeowner through a utility web interface, over the phone, or via some other method. The pre-configured link key is then sent to the Trust Center using the AMI infrastructure; see Figure 8 below and section 5.4.8.1 of [2]. This is outside the scope of the SEP 1.x specification and this white paper.

The AES-MMO hash of the installation code or serial number combined with the Media Access Control address is used as the initial *Trust Center link key*. This initial Trust Center link key is stored in the device prior to the device leaving the manufacturer. This is outside the scope of the SEP 1.x specification and this white paper.

.

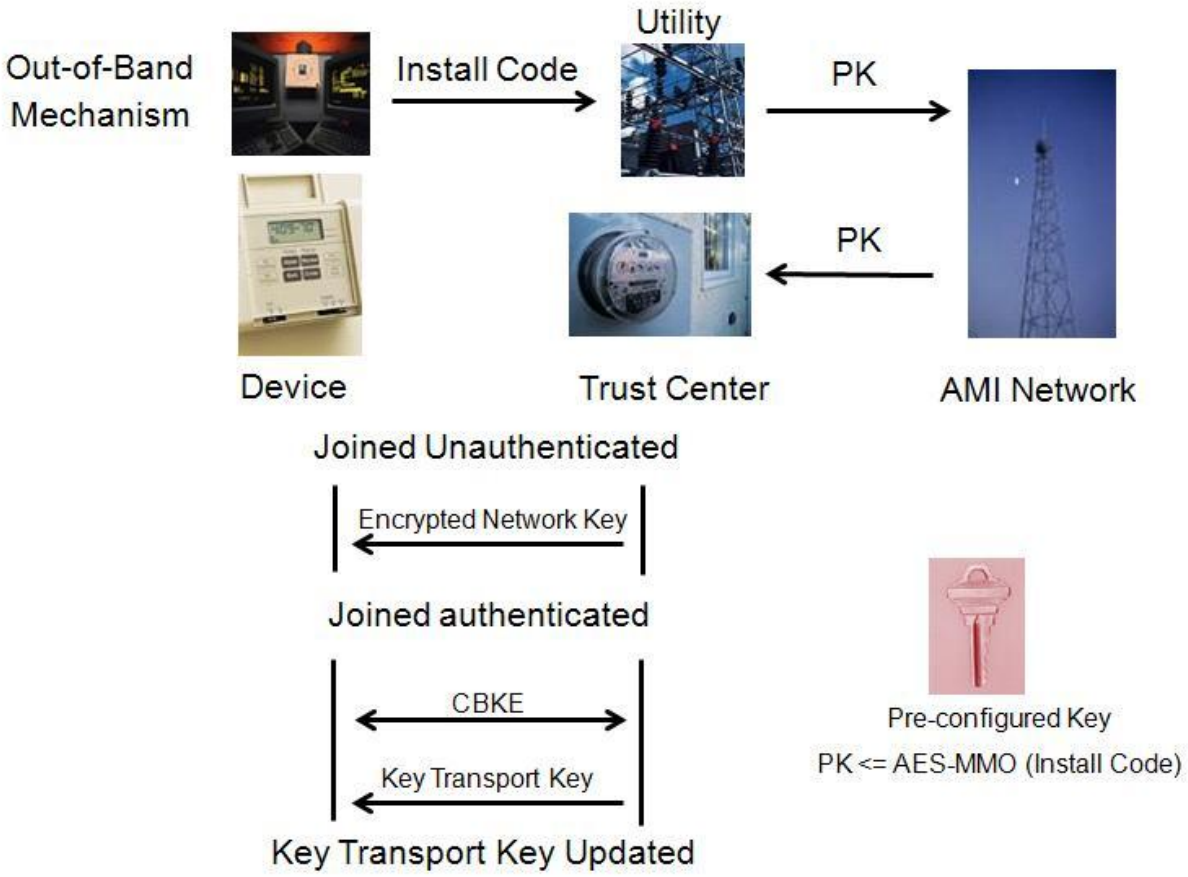

Figure 8 – Key Exchange

Authentication Procedure: The network coordinator (which is also the Trust Center) encrypts the network key, reference section 5.4.1 of [2], with the pre-configured link key and sends the encrypted network key, using the APS transport key command frame, to the joining device with the appropriate unique device ID. The network key is encrypted with the AES-MMO hash of the installation code. Because the AES-MMO hash can be computed at both the Trust Center and the joining device, it may be used as a symmetric key. AES-MMO was used as the hash as it uses the AES-128 block cipher, which is convenient for 802.15.4 devices as it is the basis for the AES-CCM frame protection and all 802.15.4 devices have AES-128 encryption as a hardware acceleration function. Only the device with the correct pre-configured link key will be able to decrypt the network key. The device then knows it has joined the proper network because the Trust Center used the proper pre-configured link key.

4.3.1 Certificate Based Key Establishment (CBKE)

After the authentication procedure is complete, the Trust Center should establish a new link key, called the Trust Center link key with the device using the certificate based key establishment (CBKE), reference section Annex C.4.2 of [2]. The new Trust Center link key serves as a unique symmetric key shared only by the Trust Center and the device. The new Trust Center link key is used for secure communications between that device and the Trust Center. Any new key transport commands (such as updating of the network key) will use this new Trust Center link key. If the Trust Center or a device determines it wants to update the link key shared with a second device, CBKE is initiated to generate a new Trust Center link key.

After joining the network a device is required to initiate key establishment using CBKE-ECMQV key agreement with the Trust Center, to obtain a new link key authorized for use in application messages. Trust Center link key generation is based on the 163 bit ECMQV key establishment suite (providing 80 bit security), referenced in Annex C.5.3.1 of [2]. The CBKE solution uses public-key technology with implicit digital certificates and root keys. Each device has a private key and an implicit digital certificate that is signed by a Certificate Authority (CA). The digital certificate includes:

- Reconstruction data for the device's public key
- The device's extended 64-bit IEEE address
- Profile specific information (e.g., the device class, network ID, object type, validity date, etc.).

Certificates provide a mechanism for cryptographically binding a public key to a device's identity and characteristics.

Trust for a CBKE solution is established by provisioning a certificate authority (CA) root key and a digital certificate to each device. A CA root key is the public key paired with the CA's private key. A CA uses its private key to sign digital certificates and the CA root key is used to verify these signatures. The trustworthiness of a public key is confirmed by verifying the CA's signature of the digital certificate. Each device generates ephemeral data that is a combination of the device identifier and the device’s static public key. The devices exchange their ephemeral data, see Figure 9, and generate a key bitstream derived from the received ephemeral data and their local identifiers. This ensures the same key is generated at both ends. From the key bitstream a message authentication is generated and the key is derived. The devices validate that they have computed the same key using a Keyed-Hashed Message Authentication Code (HMAC).

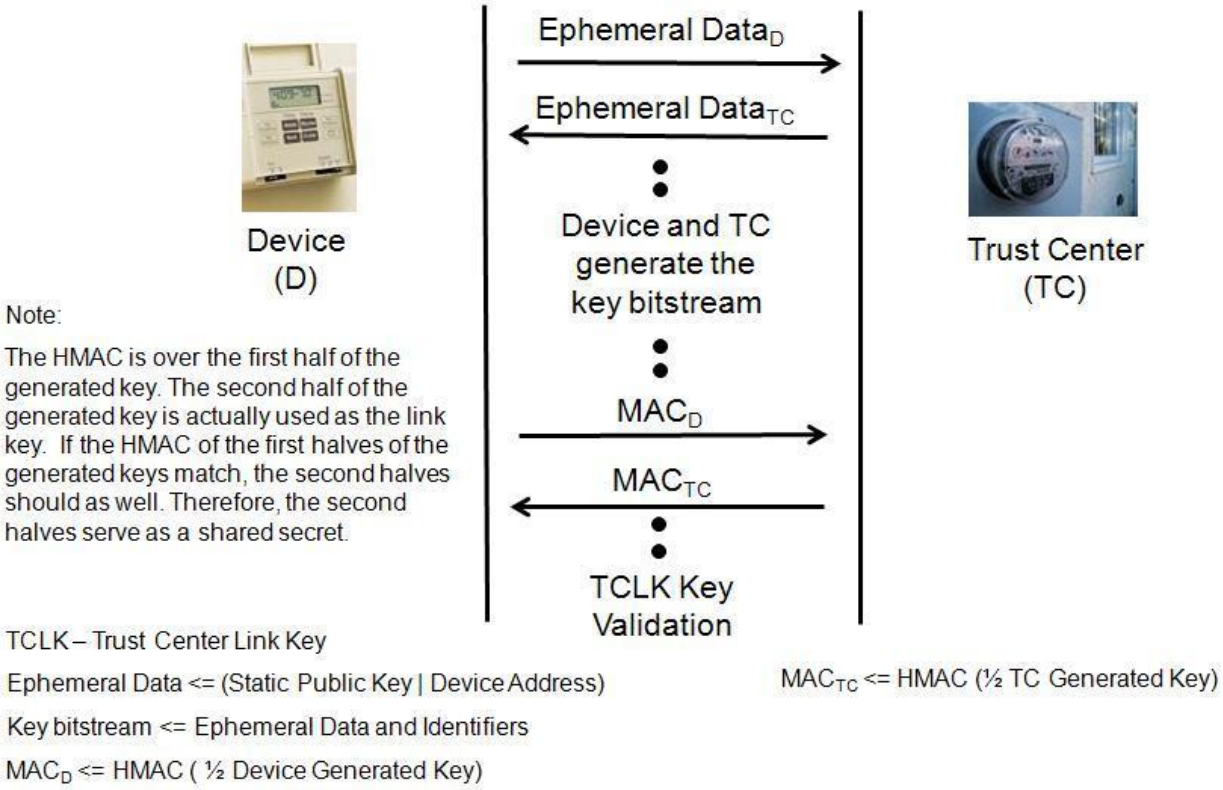

Figure 9 – CBKE and Trust Center Link Key Validation

There are no specific requirements within the SEP 1.x for the storage and handling of certificates on devices or during the manufacturing process. These need to be addressed by the manufacturer.

Recommendation: The generation, storage and handling of certificates are critical to the security of the SEP 1.x devices. Requirements and/or best practices should be developed to ensure that security is addressed.

4.3.2 SEP 1.x Keys

Table 5.13 in [2] summarizes the SEP 1.1 specification key types and usage. For example, a Demand Response message is required to be encrypted with the Application Link key while the Key Establishment Cluster messages are only required to be encrypted with the network key. Devices are tested to validate this behavior as part of the certification process to ensure messages not encrypted with the proper security level are not accepted.

Network Key: The network key is known to all devices and used to encrypt messages at the network layer (using AES 128). The network key is randomly generated by the Trust Center when the network is initiated. The network key is a common key used by all devices in the network and is transported from the Trust Center to a device when a device joins the network. Network key usage is mandatory in SEP 1.x. The current network key is held by the Trust Center and identified by a key sequence number that utilizes a two stage update mechanism:

- Generate the new key and associated key sequence number
- Switch to using the new key sequence number

The network key is periodically updated by the Trust Center using its own policy. This policy is outside the scope of SEP 1.x.

Link Keys: Link keys are special keys shared only between two communicating devices for the purpose of protecting data at the Application Support Sublayer (APS). Link key usage is mandatory in SEP 1.x. The pre-configured link key used at joining is an AES-128 symmetric key pre-configured in the joining device by the manufacturer. The pre-configured link key is provided to the Trust Center via the service provider and is derived from the installation code provided to the service provider using an out-of-band mechanism.

After a deployed device is joined to the network a link key shared with the Trust Center is dynamically established using CBKE and is used as the Trust Center link key and Application link key. The Trust Center link key is used for Trust Center operations in addition to other application payloads. The Trust Center will not accept smart energy messages from a device until it has completed CBKE.

Application Link Keys: Application link keys shared with other devices are brokered through the Trust Center. If two devices determine they require secure communications they must create a link key between them to encrypt application level payloads. The link key is only known to those two unique devices (and the Trust Center) and this prevents other devices in the network from decrypting the payload of a message they are routing. Each device sends a message to the Trust Center requesting a key with the partner device. The Trust Center, acting as a broker, determines if communications is authorized and if so, randomly generates a pair-wise key called a link key and sends it to each device with the transport key command. This link key is sent to both devices encrypted with their existing Trust Center link key. Once the transport key command is received, both devices can exchange application level messages securely by encrypting

the messages using this unique link key. Details on how link key creation is brokered through the Trust Center can be found in section 4.2.3.1 (Key Establishment) and 4.2.4 (Trust Center Role) of [24].

4.3.3 Key Updates

The Trust Center should periodically update the network and Trust Center link keys based on its policies. Currently, the policies specifying the establishment of new link keys and the time frames for updating the network and Trust Center link keys are not included in the SEP 1.x specification. Applicable requirements should be considered for the SEP 1.x specification.

Network key updates: Periodically, the Trust Center may generate a new network key. This allows the Trust Center to phase out a previous instance of the network key so that devices that are no longer on the network will not be able to perform a secure rejoin. Those devices must then perform a rejoin, which allows the Trust Center to authorize whether or not they are allowed to be on the network. The Trust Center generates the new network key, encrypts it with the old network key and broadcasts the new key to the network. The SEP 1.x specification does not associate key updates to devices leaving or joining the network; therefore SEP 1.x neither provides forward[3] nor backward secrecy[4].

Trust Center link key updates: The Trust Center may also update the Trust Center link key associated with a particular device based on the Trust Center security policy. Currently, the policy for how long a link key may be used and how often it should be updated is not included in the SEP 1.x specification. Applicable requirements should be considered for the SEP 1.x specification. Since this key is used to send application as well as stack commands and it has to be established mutually, the Trust Center cannot simply generate a new key. The Trust Center marks the old key as stale and will accept commands encrypted with the stale link key, but will discard application messages.

Rejoin Procedures: If a sleepy device misses the network key update, it can use the rejoin procedure (specified in section 5.4 of [2]) to receive the latest network key.

If a device was part of a HAN but lost connectivity or left the network and would like to return, it can also use the rejoin procedure. If the device has the current network key, it can rejoin the network using the rejoin procedure with network security. If the device

[3] Forward secrecy implies that a compromise of the current key should not compromise any future key

[4] Backward secrecy means that a compromise should not compromise any earlier key

does not have the current network key but has a Trust Center link key established using CBKE, it can use that link key to rejoin the network without network security. The Trust Center will send the device the current network key encrypted with its Trust Center link key. Devices can implement their own policies for updating pair-wise link keys with other devices (which are not the Trust Center). Currently, these policies are not included in the SEP 1.x specification. Applicable requirements should be considered for the SEP 1.x specification.

4.3.4 Cryptographic Primitives

4.3.4.1 Elliptic Curve Menezes-Qu-Vanstone (ECMQV)

ECMQV is a key exchange mechanism that provides key authentication and utilizes Eliptic Curve Qu-Vanstone (ECQV) certificates. A detailed explanation of SEP 1.x primitive establishment is provided in Annex C.5.3 of [2]. The strength of the key used in the ECMQV algorithm is of concern based on the latest NIST recommendations on key strength. The rationale for extending the transition for key agreements is similar to that for digital signatures, which is discussed in Appendix A.2 of NIST Special Publication (SP) 131a, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011, [30]. The 2013 date is an estimate and not based on specific research. Regardless, ZigBee should consider transitioning to stronger key agreement mechanisms.

Security of the ECMQV depends on the security strength of the ephemeral key pairs of the two communicating parties. SEP 1.x does not specify how the random numbers are to be generated (see 4.3.5 below). Therefore, the security strength of the key establishment may vary from one network to another and is limited by the security strength of the (pseudo) random number generation function.

AES-CCM*[5]: There are two symmetric key types used in SEP 1.x – a network key and a link key. Both keys are used as 128-bit keys for AES-CCM* encryption. The AES-CCM*

[5] Audit trail of security level 5 and the implications:

- The ZigBee Specification (053474r18) defines the attribute *nwkSecurityLevel* in section 4.3.3 (Table 4.1).
- This shows the default at level 5, which implies ENC-MIC-32, as shown in section 4.5.1.1.1 (Table 4.38).
- This gives encryption with a MIC length of 4 octets (M = 4). Note, M is **not** = 0.
- The ZigBee PRO feature set/stack profile (074855r05) document then describes the exact settings of the Security attributes and specifies in section 8.3 (Table 6) that *nwkSecurityLevel* shall be 5.
- So, as noted below: "In particular, if M is fixed and the value M = 0 is not allowed, then there are no restrictions on N, in which case the CCM* mode reduces to the CCM mode"
- Hence, AES-CCM*, as used in the ZigBee PRO stack, is identical to AES-CCM

mode of operation provides encryption and a message integrity code (MIC). AES-CCM* is used at level 5, which is an ENC-MIC mode, therefore it is equivalent to AES-CCM. This is described in Annex A and Annex B.1.2 of [24]. AES-CCM* is identical to AES-CCM with the addition of a mode that encrypts but does not authenticate. SEP 1.x only uses modes that are in the original CCM specification; it does use any of the CCM* additions. Therefore, the implementation of AES-CCM* in SEP 1.x is identical to the NIST-approved AES-CCM.

AES-MMO hash algorithm: This hash is based on the AES-128 block cipher and produces a fixed size output from a variable length input. A description of this function is in section B.6 of [24]. The AES-MMO hash algorithm is not a NIST-approved hash function. The AES-MMO hash provides, at a maximum, 64 bits of collision resistance strength. This is based on a maximum hash length of 128 bits.

This cryptographic hash is used in SEP 1.x to:

- Derive the temporary Trust Center link key from the installation code
- Hash the Trust Center key data if it is being backed up on an external device
- Sign the images sent during an OTA upgrade

HMAC MAC: Uses the AES-MMO cryptographic hash. HMAC is used in the CBKE process to ensure the integrity of the generated key.

ECDSA: Smart Energy devices may optionally support the over-the-air (OTA) bootload cluster client or server. If a smart energy device implements the OTA cluster, then APS encryption on all unicast messages must be used. Smart Energy devices that implement the client must support the Elliptic Curve Digital Signature Algorithm (ECDSA) with the AES-MMO hash function for signature verification of images. ECDSA as used in SEP 1.x is not a NIST approved method.

    - The ZigBee PRO stack is what is used by the ZigBee SEP 1.0 and SEP 1.1 Application Profiles
- CCM* is not used in 802.15.4-2003, which used CTR, CBC-MAC and CCM independently for the respective CCM* levels
- The nonce as specified in ZigBee is 13 octets long and the remainder of the counter and IV blocks are as specified in NIST SP 800-38C Appendix A (thus the octet length of the 'length length' field *q* is 2)

4.3.5 Random Number Generator

SEP 1.x does not specify how the random numbers are to be generated; this is left to the implementer. However, there is a recommendation that a deterministic RNG should conform to FIPS 140-2 (see section 4.5.4.1 of [24]). The same random number requirements should apply for the key establishment cluster as they do for all security services. Also, there may be many suitable high entropy sources dependent on the hardware.

4.3.6 Key Establishment

There are two SEP 1.x methods of key establishment: pre-installation and key agreement.

A pre-configured link key is stored in a joining device at the time of manufacture. This same key is provided to the Trust Center typically by use of an out-of-band procedure. Pre-configured link keys do not have the same security properties as dynamically-established link keys. This is because there is no mutual authentication required between the device being deployed and the Trust Center for the network it is attempting to join.

Key agreement is deriving a key based on CBKE. This is the mode used in SEP 1.x to derive the new Trust Center link key used in the operating network. Pre-configured link keys may be weak; therefore, SEP 1.x mandates that as soon as a device receives the network key, it should use the CBKE (using the network key) to establish a new link key (called the Trust Center link key) to replace the pre-configured link key. This CBKE procedure uses ephemeral data, implicit digital certificates, and HMAC.

4.3.7 Key Management

Network and link key policies for updates and modification are not defined and are left to local implementations and deployments. Section 5.4.4 of [2] requires the Trust Center to periodically update the network key. However, there is no specific requirement on this periodicity and there are no test cases for enforcing this policy.

Recommendation: Keys should be changed at regular intervals and based on the guidelines specified in NIST SP 800-57, *Recommendation for Key Management – Part 1: General, (Revision 3)* [33].

4.3.7.1 Key Storage

There are no details in the SEP 1.x specification on secure key storage, including physical key storage, within devices. There are also no requirements on memory protection of devices within the SEP 1.x specification.

Recommendation: Requirements should be developed, particularly as some classes of devices are given a higher security role because of their application function (such as the Trust Center). Compromise of an individual device would allow an outsider to view messages from that device, but compromise of the security materials in the Trust Center means the security credentials for all devices in the network would be available.

4.3.7.2 Certificate and Key Removal

Certificate revocation is not specified for the devices. However, the Trust Center can check on the utility headend for the validity of certificates on devices that are joining.

A link key can be removed by the Trust Center. For removal of the network key, all devices in the network except the device associated with the key to be removed are sent the new network key encrypted with their respective Trust Center link key. When the network switches to the new network key, the device being removed is no longer part of the network. The Trust Center link key can be removed on a given device by the Trust Center marking the key as removed or removing the device from its tables.

4.4 Layered Security

There is no protection provided at the media access control layer. Protection is provided at the network (NWK) layer and the APS. The NWK layer uses the network key and the APS layer uses the link key.

4.5 User interfaces, user interaction (security focused)

No security requirements are specified for user interfaces or user interactions in SEP 1.x, therefore user interface requirements are beyond the scope of this assessment.

4.6 Lifecycle activities: factory, device commissioning, etc.

Device commissioning is outside the scope of this assessment. There are no specific SEP 1.x requirements on the lifecycle of devices.

5 NISTIR 7628 Security Requirements

Table 2 below presents a mapping between the NISTIR 7628 cyber security requirements and the SEP 1.x specification. This table does not imply that the SEP 1.x specification fully meets the NISTIR requirements. This white paper provides analyses

on the SEP 1.x security requirements and their potential vulnerabilities and mitigations. Also included are cyber security requirements that are not defined in the SEP 1.x specification, but may be necessary to ensure that cyber security is adequately addressed in a system. Several of these system-level requirements are referenced in the SEP 1.x specification as important but outside the scope of the specification. These requirements are identified in the "Additional Implementation Requirements" column.

The SEP 1.x specification targets a diverse range of devices such as in-home displays. It would be expected that assets have additional requirements beyond those pertaining to SEP 1.x to fulfill the requirements identified in the "Additional Implementation Requirements" column.

Table 2 – NISTIR 7628 to ZigBee SEP 1.x Mapping

NISTIR Requirement Identifier	NISTIR Requirement Name	NISTIR Category[6]	SEP 1.x References	Additional Implementation Requirements
SG.AC Access Control				
SG.AC-1	Access Control Policy and Procedures	GRC		**SEP 1.0** Section 5.4.5 **SEP 1.1** Section 5.4.5
SG.AC-14	Permitted Actions without Identification or Authentication	UTR		**SEP 1.0** Annex B **SEP 1.1** Annex B
SG.IA: Identification and Authentication				

[6] The NISTIR 7628 identifies three types of security requirements: governance, risk, and compliance (GRC), common technical (CTR), and unique technical (UTR).

NISTIR Requirement Identifier	NISTIR Requirement Name	NISTIR Category[6]	SEP 1.x References	Additional Implementation Requirements
SG.IA-5	Device Identification and Authentication	UTR	**SEP 1.0** Section 2.1.1 Section 5.4.1 Section 5.4.2 Section 5.4.7 Section 5.4.8.1 Section 5.5 Annex C Annex F **SEP 1.1** Section 2.1.1 Section 5.4.1 Section 5.4.2 Section 5.4.7 Section 5.4.8.1 Section 5.5 Annex C Annex F	
SG.CM: Configuration Management				
SG.CM-8	Component Inventory	UTR		**SEP 1.0** Section 5.4.8.2.1 **SEP 1.1** Section 5.4.1.1
SG.SC: Smart Grid Information System and Communication Protection				
SG.SC-8	Communication Integrity	UTR	**SEP 1.0** Annex C.2.3 Annex C.4.2.2.7 **SEP 1.1** Annex C.2.3 Annex C.4.2.2.7	
SG.SC-9	Communication Confidentiality	UTR	**SEP 1.0** Section 5.4.7 **SEP 1.1**	

NISTIR Requirement Identifier	NISTIR Requirement Name	NISTIR Category[6]	SEP 1.x References	Additional Implementation Requirements
			Section 5.4.7	
SG.SC-11	Cryptographic Key Establishment and Management	CTR	**SEP 1.0** Section 2.1.2 Section 5.4.4 Section 5.4.5 Section 5.4.7 Annex C Annex F **SEP 1.1** Section 2.1.2 Section 5.4.4 Section 5.4.5 Section 5.4.7 Annex C Annex F	
SG.SC-12	Use of Validated Cryptography	CTR	**SEP 1.0** Section 5.4.6 **SEP 1.1** Section 5.4.6	
SG.SC-15	Public Key Infrastructure Certificates	CTR	**SEP 1.0** Section 5.4.5 Section 5.5.5 Annex C.2.5 Annex C.3.1 Annex C.4.2 Annex C.5 **SEP 1.1** Section 5.4.5 Section 5.5.5 Annex C.2.5 Annex C.3.1 Annex C.4.2 Annex C.5	
SG.SC-20	Message Authenticity	CTR	**SEP 1.0** Annex C.4.2.3	

NISTIR Requirement Identifier	NISTIR Requirement Name	NISTIR Category[6]	SEP 1.x References	Additional Implementation Requirements
			SEP 1.1 Annex C.4.2.3	

6 Potential Vulnerabilities, Mitigations, and Best Practices[7]

This section includes the impacts and proposed mitigations to the identified potential vulnerabilities in the SEP 1.x specification. These vulnerabilities were identified in previous security reviews such as the CSWG assessment [12], the CMU assessments [14, 15], and the Honeywell assessment [34]. Section 6.1 includes vulnerabilities, impacts, and mitigations for the requirements included in the SEP 1.x specification. Section 6.2 includes vulnerabilities and mitigations for implementation specific requirements that are outside the scope of the SEP 1.x specification, but are applicable to ensuring the security of the operational system. Section 6.3 includes best practices. Section 6.4 identifies security functionality that is outside the scope of the SEP 1.x specification and needs additional security analysis.

6.1 SEP 1.x Specification Vulnerabilities, Impacts, and Mitigations

The material in this chapter is consolidated from the reviews performed by the SGIP CSWG, CMU, Robert Cragie, and Honeywell. Honeywell added to the assessments performed by CMU, the CSWG, and Robert Cragie.

Deprecated Cryptographic Algorithms: The CSWG identified an issue relating to the use of deprecated cryptographic algorithms. Although these deprecated cryptographic algorithms do not necessarily make the SEP 1.x profile insecure, they do have security implications. NIST has deprecated the use of cryptographic algorithms that provide less than 112 bits security. The ECMQV protocol used in SEP 1.x provides 80 bits of security. NIST recommends that data owners have the responsibility to protect their data with adequate protection and 80 bit protection can be used until 2013 with the acceptance of some risks [30]. During the time that the SEP Profiles 1.0 and 1.1 were developed, this was permissible. However going forward, from 2013-2030 the minimum symmetric key strength should be 112 bits. This means that the ECC private key should

[7] The majority of the content in this chapter was developed by the Honeywell team – Himanshu Khurani, Tom Markham, and Apurva Mohan.

be at least 224 bits in length. With today's computing power, 80 bit security is relatively secure. Because HAN devices are typically installed for a number of years (often 15 or more years) future computing power can make 80 bit protection vulnerable to brute force attacks.

Link Key Vulnerability: Any outsider who obtains a link key will be able to decrypt transactions protected at the APS layer and masquerade as a genuine application participant. Getting access to a cryptographic key is vulnerability for all cryptographic keys – it is not unique to SEP 1.x.

Network Key Vulnerabilities: Any outsider who obtains the network key will be able to decrypt transactions protected at the network layer. Application layer payloads will still be protected by the application link key. The outsider can also masquerade as a genuine network participant. Getting access to a cryptographic key is a vulnerability for all cryptographic keys – it is not unique to SEP 1.x.

6.2 Implementation-Specific Vulnerabilities and Mitigations

This section includes potential vulnerabilities when SEP 1.x is implemented. These potential vulnerabilities are in the operational environment and not specific to the SEP 1.x specification.

6.2.1 Access control

Background: In SEP 1.x all devices are given the network key upon joining the network (see section 5.4.1 of [2]). The network key is updated periodically but updates are not linked to devices joining or leaving the network. There is no specific reason a device leaving a network should force a network key update; that would precipitate that device not being able to simply rejoin. This may be desired as a security policy but there is no rationale for generally specifying this requirement. Upon joining a network, the Trust Center provides the network key to the device encrypted with the device's pre-configured link key. During later updates, the new network key is encrypted with the current network key. The SEP 1.x specification leaves the key update policy to be decided locally by the Trust Center (see section 5.4.4 of [2]).

The rejoining procedure described in section 5.4.2 of [2] states that if a device has the current network key it can rejoin a secured network.

Issues and vulnerabilities: If a device has the network key, it can receive all the subsequent network keys and listen to messages encrypted with the network key. This

is possible because of the current mechanism of broadcasting a new network key secured with the old network key.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures.

Mitigations and best practices: Access control to the network needs to be strong and the Trust Center should be able to decide when a suspected malicious device should be forced out of the network or when a suspected malicious device should not be allowed to join or rejoin the network. This can be handled by using proper access control policies in the Trust Center.

When a device that is currently in the network is detected as malicious, the Trust Center should apply policies to remove a device from the network. This should include de-registration from the network (see section 5.4.2.2.2 of [2]) and sending the device the leave command in section 5.4.4 of [2])[8]. Consequently, the suspected device will not be able to communicate with any other device on the application level. The Trust Center should then perform a unicast update of the network key followed by a broadcast switch key as described in section 5.4.7.3 of [2] but used in a different context. This will provide forward secrecy to the network. It will also prevent the device from rejoining the network.

A-priori detection of malicious devices is a hard problem and this includes anomaly detection algorithms to detect malicious or misbehaving devices using a range of undesirable behavior. This is a significant research area. Section 5.4.7.3 of [2] describes one case to deal with a malicious device. The Trust Center may implement either blacklisting or whitelisting to ensure only authorized devices join the network or remain on the network.

Some other relevant access control policies for the UE-HAN and CP-HAN are described below. As with all policies, these may be subverted by a determined adversary.

UE-HAN: The registration portal should authenticate a device and a user registering a device. This may include verification of account information and device serial number.

[8] Ideally this should be in the respective stack profiles. The features of high security mode (use of SKKE key establishment, entity authentication) were considered unnecessary for typical ZigBee networks. Standard security was specified for the ZigBee PRO stack profile with additional requirements for the common security profile. Therefore, specified in SEP 1.x is the basic standard security profile with some additions, such as mandating the use of Trust Center link keys. SEP 1.x also uses the Key Establishment Cluster, which is not part of the ZigBee Specification and this adds CBKE using the SEP 1.x application profile clusters.

This may prevent an unauthorized device from joining the UE-HAN and obtaining the network key.

CP-HAN: CP-HAN operation is not described in the SEP 1.x specification and may differ from vendor to vendor. A best practice is for the Trust Center to provide a means for the customer/installer to validate the identity of a device attempting to join the network (e.g., serial number, device description) before the pre-configured link key is used to distribute the network key to the device.

Implementation of the policies described above will help ensure that any device that leaves the network will not be allowed to rejoin the network using the rejoin procedure specified in section 5.4.2 of [2]. If a device on the blacklist (or not on the whitelist) tries to join the network using the registration process, the Trust Center should not respond to the join request.

If backward secrecy is desired in the network, then the Trust Center should update the network key just before a new device joins the network if the Trust Center is notified of devices that will be joining the network.

6.2.2 Malicious device joining the network

Background: The SEP 1.x specification states that once a device is suspected to be malicious, it may be sent a network leave command and it may be forced off the network by having the Trust Center send a unicast update of the network key specified in section 5.4.7.3 of [2] followed by a broadcast switch key. This may be a result of the device failing CBKE because of a bad certificate.

Issues and vulnerabilities: Using the procedure in section 5.4.7.3 of [2] will alert the device that it is identified as malicious. The device may obey the leave command to leave the network but use the rejoin procedure by using the network key to rejoin the network, thus effectively wiping out its detection in the network. Devices that are identified as malicious by other techniques may use this method (refer to section 6.2.5 below).

Due to this potential vulnerability, a misbehaving or compromised device may evade detection and continue to either disrupt the network or capture sensitive network information. The customer may be impacted by network disruption by misbehaving devices or application payload data may be compromised.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures.

Mitigations and best practices: The Trust Center should update the network key when it has sent a leave command to prevent a potentially malicious device from rejoining the network using the old network key. Section 6.2.1 above describes how a Trust Center should maintain a list of blacklisted/whitelisted devices. The Trust Center should note the current known status of a blacklisted device like ‘joined network’, ‘left network’ etc. For a blacklist, the Trust Center should update the details of the device once it changes status but should not delete a suspected device’s entry from the table. The Trust Center should refer to this table before authorizing a device to join or rejoin the network. An entry from the malicious devices table should only be removed by procedures described in section 6.2.5 of this document. For a whitelist, the Trust Center should remove the device entry from the list.

6.2.3 Devices leaving the network

Background: When a device leaves the network, the Trust Center should delete its link key.

Issues and vulnerabilities: SEP 1.x does not describe the condition when the Trust Center identifies that a device has left the network. If a device is sleeping for an extended period or its battery is dead, the assumption is that the device has not left the network.

Mitigations and best practices: The Trust Center should only delete the link key of a device when it leaves the network. This can be more clearly defined based on explicit requests and then an inactivity period in relation to known sleep periods/key updates. Clearly defining what constitutes a leave, knowledge of sleepy devices, and a comprehensive network key update policy will provide the best mitigation.

6.2.4 Registering fake devices

Background: Before a Trust Center allows a new device into a HAN, the device installation code and other profile specific details must be provided to the Trust Center using an out-of-band mechanism, as specified in SEP 1.x. The utility or the web portal will forward this information to the Trust Center. SEP 1.x does not architect the mechanism and allows for different topologies for the smart energy network.

Issues and vulnerabilities: SEP 1.x does not describe a specific mechanism that may lead to implementation choices that are not secure. It is the responsibility of the manufacturer and the utility to specify a secure mechanism.

By registering fake devices on the network, adversaries can cause the home energy devices to behave in an undesired fashion by sending fictitious command messages. They can also disrupt the network operations or compromise application payload data.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures and SG.IA-5 Device Identification and Authentication.

Mitigations and best practices: The out-of-band mechanism that provides the registration information to the Trust Center should be secure, e.g., web login, security questions, ALG device serial number.

6.2.5 Detecting malicious devices

Background: SEP 1.x defines certain behavior from devices as malicious (see section 5.4.7.3 of [2]).

Issues and vulnerabilities: There are many types of behaviors that can be described as potentially malicious but they are not specified in SEP 1.x. Currently, it is very difficult to accurately detect a malicious device.

If malicious or compromised devices are not detected, they can continue to harm the network or compromise application payload data.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures.

Mitigations and best practices: The Trust Center should implement policies and algorithms to detect suspicious behavior and monitor behavior of devices in the network based on their interaction with the Trust Center. As noted above, detecting suspicious behavior is a research area.

6.2.6 Inter-Personal Area Network (PAN) communication

Background: Inter-PAN communication allows ZigBee devices to perform limited, insecure, and possibly anonymous exchanges of information with devices in their local neighborhood without having to form or join the same ZigBee network. The mandate for this feature comes from the Energy Management/Smart Energy market requirement to send pricing information to very low cost devices. The particular data exchange required by the Smart Energy Application Profile is the request for anonymous public energy pricing information.

Issues and vulnerabilities: Inter-PAN communication does not require any security, which means that a device in one HAN can talk to devices in any other HAN. Because

this can have a serious impact on the HAN, an adversary can create a new HAN and communicate with a consumer HAN without any security requirements. The adversary could compromise application payload data and cause control devices to misbehave causing problems.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures, SG.IA-5 Device Identification and Authentication, SG.AC-14 Permitted Actions without Identification or Authentication.

Mitigations and best practices: The inter-PAN mechanism is part of the ZigBee specification but is not required to perform any core functionality. Therefore, this mechanism should be limited to sending pricing information.

6.2.7 Key Updates

Background: Once a device joins a ZigBee network it is expected to perform a CBKE procedure (see Annex C.4.2 of [2]) to establish an application link key with the Trust Center. It the device does not initiate CBKE then the Trust Center is told to initiate CBKE. [2] does not put a time limit on a device to complete the CBKE procedure but leaves it to the HAN policies.

Issues and vulnerabilities: Section 5.4.7.3 of [2] states that a device that never performs the CBKE to establish an application link key may be sent a leave command. This is only done for non-security reasons.

Applicable NISTIR 7628 requirement: SG.SC-11: Cryptographic Key Establishment and Management.

Mitigations and best practices: The Trust Center policy should distinguish between devices that never attempt to establish a link key in a reasonable time period (which probably is suspicious) and devices that fail CBKE. The latter may be because the device is on the wrong network - this is not malicious. A “reasonable time” should be defined in policy. It may also be prudent to update the network key, although that should be a policy decision.

Section 5.4 of [2] describes the procedures to be followed by the Trust Center to establish and update the application and Trust Center link keys. Section 5.4.7.3 of [2] discusses the action a Trust Center should take when a device does not establish a Trust Center link key. Since a device does not have access to the Trust Center link key before it joins the network and after it leaves the network, a device can only communicate on the application level when it is part of the network. Also, after a device

has been told to leave a network, the Trust Center should check if the device had established any pairwise link keys and if so it should invalidate them. This will ensure that a device cannot communicate with other devices once it leaves the network.

6.2.8 Malicious insiders with access to the network key

Background: Once a device joins a ZigBee network, it is provided the network key. A malicious individual may be able to read the network key off the device by physical tampering or cryptanalysis of the network communication.

Issues and vulnerabilities: In the smart energy profile, a few application level cluster messages are encrypted by only the network key (see table 5.13 in [2]). Attackers who have access to the network key can manipulate these messages. These attackers can cause disturbances in the network communication and operation of the HAN and between the Trust Center and the HAN.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures.

Mitigations and best practices: Security policies and procedures should be defined and implemented to protect against the leakage of a network key through device compromise or cryptanalysis. For example, Annex D of [2] mentions the use of a tamper bit to be set if a device is suspected to be tampered. Additionally, physical tamper detection measures may be used to detect device tampering. Strong network key update policies, strong installation codes, and strong link key protection should be implemented.

6.2.9 HAN Security Policies

Section 5.1 of [2] describes two types of HANs; one of which is enabled by the utility and the other is owned by the customer. ZigBee devices are expected to join one of these networks depending on what network topology is chosen. If the topology chosen for a smart energy network contains a UE-HAN and a CP-HAN, then each HAN needs to define a security policy.

Applicable NISTIR 7628 requirement: SG.AC-1 Access Control Policy and Procedures.

6.2.10 Boot-load Cluster Upgrade

The ZigBee bootload cluster detailed in Annex D.8 of [2] provides a standard method for over the air upgrading of devices. This requires the use of application link keys to transmit the image over the ZigBee network and validation of the digital signature of the image by a device prior to using the image. These specifications are appropriate for

protection of bootloading new images. However, the following items are not addressed by the bootload functionality and should be considered by implementers:

1. The mechanism for transporting and storing a new firmware image prior to it being transmitted on the ZigBee network is not specified and could be insecure. This should be evaluated for vulnerabilities by implementers. The image cannot be tampered with because it contains a digital signature but exposure of the image may allow its analysis for attack vectors.

2. The storage of the bootload image is often in external flash to the ZigBee device. If the image is store unencrypted in the external flash, it may be subject to compromise. Implementers should consider encrypting the stored image.

6.3 Best Practices

This section includes best practices for the SEP 1.x specification. These are not necessarily vulnerabilities, but are recommendations to enhance the cyber security of an implementation.

6.3.1 Trust Center

The Trust Center in a ZigBee HAN has the responsibility of network coordination, network security, and network management. As such, the Trust Center is the central device in the ZigBee network. As described above, most of the vulnerabilities in the ZigBee network can be mitigated or minimized by adding compensating controls and mitigations in the Trust Center. Also, the security of the Trust Center itself is an important issue and needs to be considered. A secure and robust Trust Center is needed to implement security policies and mitigation strategies that will ensure that certain vulnerabilities in the network and protocol can be mitigated.

Most of the vulnerabilities identified in this document and the referenced security analyses documents can be addressed by proper usage of the ZigBee specifications, SEP 1.x specification, and deployment of a robust, extensible, and flexible Trust Center. The Trust Center should implement the various policies and best practices recommended to harden the SEP 1.x security. A flexible and extensible approach will make it possible to further improve security by implementing additional measures when new security vulnerabilities are identified.

6.3.1.1 Trust Center Key Management Policies

The Trust Center should have specific policies on key update periodicity and devices in a network should expect key updates at this frequency from their Trust Center. Specific events may also be specified to trigger a key update. These need to be written as

requirements and not as best practices for the networks. There are disparate policies as to how long the permit join flag should be set due to operational conditions for the distribution and management of HAN devices. A Trust Center policy should outline a specific process that limits the amount of time the permit flag is set on. If the permit joining flag is left on for a long time, it will create an opportunity for rogue devices to join a HAN and potentially create problems or compromise data.

Section 6.2 above describes some potential key update vulnerabilities that may be used in developing key update policies for the Trust Center. Certain requirements such as forward and backward secrecy, compromise of cryptographic keys, and inclusion of sleepy devices should be considered in defining key management policies for Trust Centers. A balance between operational constraints and network and cryptographic security should be considered in defining key management policies.

6.3.2 Link key based on installation code

Background: SEP 1.x recommends that the installation code be random. Upon joining the network the network key is sent to the device encrypted with the pre-configured link key that is derived from the installation code on the device using the AES-MMO hash algorithm according to the procedures described in section 5.4.8.1 of [2]. There is no salt to the AES-MMO hash. The installation code is chosen by the device manufacturer and may be a 48, 64, 96 or 128 bit number with a 16 bit CRC. In the absence of proper randomization of the installation code, an adversary can study the pattern of installation codes and try to guess the code pattern. He can then use the hash to derive the link key and try to guess the encrypted network key.

Issues and vulnerabilities: The installation code can be as short as 48 bits. This short installation code may be subject to a brute force attack by an attacker to derive the link key and later capture the network key. The attacker could then use the network key to access application payload data or perform operations that any device in the network can perform.

Applicable NISTIR 7628 requirement: SG.SC-11: Cryptographic Key Establishment and Management.

Best practices: The choice of the installation code is left to the device manufacturer and is outside the scope of the SEP 1.x specification. The installation code should be a 128 bit random number conforming to the FIPS140-2 standard. This will make it difficult for an adversary to guess the pre-configured link key or the network key. Randomness will increase the entropy and 128 bits will make a brute force attack more difficult.

6.3.3 Key domain overlaps

Background: SEP 1.x uses two types of keys, the network key and the application link key. The link key is implemented at the application layer to protect data that needs a higher level of protection. Some data were not considered significant from a security perspective and therefore were not protected with the link key. The overlap occurs when a Trust Center link key, which is used for network access, is also used as an application link key for application layer security. This is not inherently insecure, but is a sharing and overlapping of security domains.

Applicable NISTIR 7628 requirement: SG.SC-11 Cryptographic Key Establishment and Management.

Best practices: Key domain overlaps is not a security issue in itself but exposes other domains to the compromise of a cryptographic key in one domain. Generally key domains should not overlap and each domain should have an independent domain key.

6.3.4 Certificate management

Background: For ZigBee networks, Certicom (a division of RIM) is the CA and issues certificates for devices and smart meters. Since there is a single certificate provider there are no issues related to creating a chain of trust to verify the certificate. Each device has its own certificate and uses it to establish an application link key with the Trust Center in Annex C of [2].

Applicable NISTIR 7628 requirement: SG.SC-15 Public Key Infrastructure Certificates.

Best practices: Although it is a good security practice to avoid certificate overlaps between different networks, it is not a security flaw. However, avoiding certificate overlap is difficult to support with long-term device certificates. Devices that are part of multiple networks will have multiple certificates. This is not addressed in the SEP 1.x specification. Devices that are part of multiple networks will require a new set of guidelines, best practices, and specifications.

6.4 Functions Outside the SEP1.x HAN Analysis Scope

There are several functions that are outside the scope of the security functionality documented in the SEP 1.x specification. Following is a partial list of these functions:

- Customers privacy in the CP-HAN,
- Restricted physical access to the meter,
- HAN devices cannot penetrate the AMI,

- Plug in vehicles (or anything with potentially special charging rates or energy charging reservation), and
- Distributed energy resources that allow devices in the HAN to put energy back into the grid.

The addition of these services outside of what was analyzed in this white paper should be subject to future security reviews prior to deployment.

This following two subsections identify additional cyber security threats for the SEP 1.x HAN. They are documented to provide a more complete overview of the cyber security threats for the SEP 1.x environment. Some of these out-of-scope threats may be addressed by other working groups (e.g., AMI CSWG[9]).

6.4.1 ZigBee Radio Physical Tampering Exploitation

The physical security of ZigBee devices is vendor dependent and outside the scope of the SEP 1.x specification. Utilities and customers must acknowledge at least some level of risk that is due potentially to physical access/tampering of a SEP 1.x HAN device. As an example of a related published physical tampering ZigBee exploit, ZigBee radio keys have been extracted from the RAM of a particular commercial ZigBee radio chip [32]. This published work indicates that the vulnerability may be similarly leveraged to exploit other makes and models of commercial ZigBee radios. In general, the work by Goodspeed has demonstrated the proof of concept feasibility (if not practicality) of ZigBee radio compromise via physical access.

As discussed earlier, once access to SEP 1.x cryptographic keys is acquired, an adversary can sniff HAN traffic, masquerade as a legitimate SEP 1.x device or application, and initiate denial of service attacks. In addition, due primarily to swap and cost constraints, there is little or no separation/isolation of processes on a ZigBee device. Therefore, an adversary that has acquired access to one component of a ZigBee device can likely obtain access to other applications/functions on the device in section 5.4 of [2].

While the likelihood and ease for exploitation via physical tampering of ZigBee radios is subject to debate, there is clearly a need for utilities to take some rudimentary protective measures. Most current smart meters have some type of physical tampering detection. Because of the potential for tampering, utilities should not trust HAN devices and should view any messages from them as suspect.

[9] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGAMI

6.4.2 AMI/HAN Interface Exploitation

The interface between the AMI and SEP 1.x protocol stacks is implemented at the application layer and, therefore, uses application layer protection mechanisms to protect the two stacks. Specifically, message format checks and buffer overflow prevention will help isolate the two stacks and help thwart attacks originating in the HAN and directed at the AMI network (and vice versa). Where the application layer interface between the two stacks is vendor-dependent, there is the possibility of vulnerabilities being introduced in the smart meter firmware[10].

7 Conclusion

Load control capabilities in Home Area Networks (HANs) are an integral part of the smart grid and energy efficiency modernization efforts currently underway. Like other smart grid systems, HANs are vulnerable to cyber attacks and adequate security measures are needed. The Zigbee Smart Energy Profile 1.0 and Smart Energy Profile 1.1 (collectively referred to in this white paper as SEP 1.x) present a communication framework for HAN devices along with a security framework.

The Trust Center in a ZigBee HAN has the responsibility of network coordination, network security, and network management. As such, the Trust Center is the central device in the ZigBee network. Most of the vulnerabilities identified in this white paper and the referenced security analyses documents can be addressed by proper usage of the ZigBee specifications, SEP 1.x specification, and deployment of a robust, extensible, and flexible Trust Center. A flexible and extensible approach will make it possible to further improve security by implementing additional measures when new security vulnerabilities are identified.

[10] The AMI CSWG will have more guidance on the protection of the AMI/HAN interface in its assessment of smart meter security.

8 References

(Note: NIST publications are available at csrc.nist.gov and Certicom publications are available at www.secg.org)

1. ZigBee Document 075356r15, ZigBee Alliance, *ZigBee Smart Energy Profile Specification 1.0*, ZigBee Profile 0x0109, Revision 15, December 1, 2008

2. ZigBee Document 075356r16, *ZigBee Alliance, ZigBee Smart Energy Profile Specification 1.1, ZigBee Profile 0x0109, Revision 16*, Version 1.1, March 23, 2011

3. ZigBee Document 085195r02, ZigBee Alliance, *ZigBee PRO Trust Center Best Practices, Revision 1*, November 25, 2008

4. NIST SP 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST, May 2004

5. Federal Information Processing Standards Publication (FIPS) 197, *Advanced Encryption Standard (AES),* NIST, November 26, 2001

6. *Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography,* Certicom Research, May 21, 2009 Version 2.0

7. *Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters*, Certicom Research, January 27, 2010 Version 2.0
8. *ECQV (80 bit) Implicit Certificates: Standards for Efficient Cryptography: SEC 4 (draft) ver 1.1r1: Elliptic Curve Cryptography*, Certicom Research, June 9, 2006

9. *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison and San Diego Gas & Electric Company*, California Public Utilities Commission, July 29, 2011

10. *Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review, CSWG Standards Review Report, ZigBee Smart Energy Profile Specification 1.0, Document 075356r15*, 2008, Smart Energy Profile

Specification Version 1.0, July 18, 2011

11. *Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review, CSWG Standards Review Report, ZigBee Smart Energy Profile Specification 1.1, Document 075356r16ZB*, 2008, Smart Energy Profile Specification Version 1.1, July 18, 2011

12. *ZigBee SEP 1.0 Security Analysis*, Robert Cragie

13. *Smart Meter Texas, SMT and HAN Technical Orientation for Competitive Retailers briefing*, January 7, 2010

14. *085007r00ZB ZSE-SE Security External Audit Report, ZigBee SE Profile Security Review Report, (Rev 1.1) for ZigBee Document 075356r12ZB*, Aug 5, 2008, Carnegie Mellon University

15. *Sep 1.x 085008r01ZB_ZSE-SE_security_review_errata, ZigBee SE Profile Security Review Report Changes (Version 1.0 to 1.1),* Revision date, Aug 5, 2008, Carnegie Mellon University

16. *CMU SE Security Review Response, CMU Security External Audit Report (085007r02),* ZigBee Alliance, March 2009

17. NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised),* March 2007, NIST

18. NIST SP 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST, May 2004

19. FIPS Pub 197, *Advanced Encryption Standard (AES),* , US Department of Commerce/NIST, November 26, 2001

20. FIPS Pub 198, *The Keyed-Hash Message Authentication Code (HMAC)* , US Department of Commerce/NIST, March 6, 2002

21. *ZigBee 075390r04, ZigBee Alliance, ZigBee SE Profile: Protocol Implementation Conformance (PICS) Proforma*, December 2008

22. ZigBee Document 094980r03, ZigBee Alliance, *ZigBee Smart Energy Test Specification*, April, 2009

23. ZigBee Document 08006r03, ZigBee Alliance, *ZigBee-2007 Layer PICS and Stack Profiles, Revision 03*, June 2008

24. ZigBee Document 053474r18, ZigBee Alliance, *ZigBee PRO Specification*, June 18, 2009

25. ZigBee Document 095264r17, ZigBee Alliance, *ZigBee Over-the-Air Upgrading Cluster*, Version 0.7, March 14, 2010

26. ZigBee Document 095284r06, ZigBee Alliance, *SEP 1.1 Over the Air Bootload Cluster PICs [protocol implementation conformance statement],* 07 October 2010

27. ZigBee Document 08006r03, ZigBee Alliance, ZigBee-2007 Layer PICS [protocol Implementation conformance statement] and Stack Profiles, Revision 03, June 2008

28. ZigBee document 064309r04, ZigBee Alliance, *Commissioning Framework*. (Note: currently, there are no known SEP 1.x deployments using the Commissioning Framework

29. 802.15.4-2003, IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) (Note: This is a deprecated version of the IEEE 802.15.4 specification (current version is 2006))

30. NIST SP 800-131a, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST, January 2011

31. NISTIR 7628, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements; Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid; Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References*, NIST, August 2010

32. T. Goodspeed, “Extracting Keys from Second Generation ZigBee Chips,” Black Hat USA 2009 (available at http://www.blackhat.com/presentations/bh-usa-09/GOODSPEED/BHUSA09-Goodspeed-ZigBeeChips-PAPER.pdf)

33. NIST SP 800-57, *Recommendation for Key Management – Part 1: General,*

(Revision 3), NIST, May 2011

34. A. Mohan, H. Khurana, T.Markham, *ZigBee Smart Energy Profile 1.x - Security Analysis and Mitigations*, *Draft Version 0.11,* Sept. 27, 2011

9 Acronyms

AES	Advanced Encryption Standard
AES-CCM	Advanced Encryption Standard – Counter with CBC MAC
AES-MMO	Advanced Encryption Standard - Matyas-Meyer-Oseas
ALG	Application Layer Gateway
AMI	Advanced Metering Infrastructure
APS	Application Support Sublayer
CA	Certificate Authority
CBC-MAC	Cipher Block Chaining with Message Authentication Code
CBKE	Certificate Based Key Establishment
CMU	Carnegie Mellon University
CP-HAN	Consumer Private – Home Area Network
CPUC	California Public Utility Commission
CRC	Cyclical Redundancy Check
CSWG	Cyber Security Working Group
CTR	Counter
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
ECQV	Elliptic Curve Qu-Vanstone
EMS	Energy Management System
ENC-MIC	Encryption Message Integrity Code
ERCOT	Electric Reliability Council of Texas
ESB	Enterprise Service Bus
ESI	Energy Services Interface
ESP	Energy Services Portal
HAN	Home Area Network
HMAC	Keyed-Hashed Message Authentication Code
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers

IOU	Independent Operating Unit
NAN	Neighborhood Area Network
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NWK	Network
OTA	Over The Air
PAN	Personal Area Network
PG&E	Pacific Gas and Electric
PK	Pre-Configured Key
RAM	Random Access Memory
SCE	Southern California Edison
SDG&E	San Diego Gas and Electric
SEP	Smart Energy Profile
SMT	Smart Meter Texas
TCLK	Trust Center Link Key
TDSP	Transmission/Distribution Service Provider
TWG	Technical Working Group
UE-HAN	Utility Enabled – Home Area Network