# National Electric Sector Cybersecurity Organization Resource (NESCOR) and Cyber Security Working Group (CSWG)

---

## Smart Energy Profile (SEP) 1.x Analysis

**9/1/2011**

# Acknowledgments

The following individuals are members of this working group:

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 Yan, Will Arensman, Larry Korhmann, Wendy Al-Mukdad, Alan Greenberg, Roger Levy, Charles McParland, Christopher Villarreal, Apurva Mohan, Justin Searle, Akhlesh Kaushiva, John Sucec, and Alan Rivaldo, Roger Levy

These individuals have contributed their time and technical expertise to ensure that the content of this technical white paper is accurate. In particular, the ZigBee Alliance has provided this working group access to all the documents that we have needed.

# Table of Contents

# 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 revisions of the ZigBee Smart Energy Profiles (SEP). This includes ZigBee SEP 1.0 and 1.1. These are referred to as ZigBee SEP 1.x in this document. To assist utilities, regulators, and integrators who are deploying and configuring ZigBee SEP 1. x in field devices, NESCOR and the Cyber Security Working Group (CSWG) are developing a technical white paper that provides guidance on the use of both profiles. There are three deliverables for this task:

1) Annotated outline - 09/01/11

2) Draft technical white paper – 09/30/11

3) Final version of the technical white paper that incorporates comments from all interested parties. – 10/31/11

## 1.1 Scope

In this technical white paper, the security gaps and potential vulnerabilities of the ZigBee SEP 1.x will be identified and documented. Security reviews done in the past such as the CSWG review, Carnegie Mellon University (CMU) review, and other independent reviews will be consulted. Security requirements will also be derived from the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* document. An independent security review of the ZigBee SEP 1.x specifications will also be done by the team and additional security gaps and vulnerabilities, if any, will be identified. The difference between the two versions of the ZigBee SEP specifications will be assessed to consider the impact of these security gaps on each one of them. Finally, recommendations will be made on how the ZigBee SEP 1.x profile should be implemented in deployments.

The approach taken in this 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 ZigBee 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 paper will identify compensating controls and best practices to mitigate or minimize the identified risks. Based on these compensating controls and best practices, the paper will make recommendations on how the ZigBee SEP 1.x profile should be deployed. Ideally, these compensating controls and best practices will be specified in such a way that they are compliant with ZigBee SEP 1.x and can be implemented in deployed or to-be-deployed ZigBee SEP 1.x based HANs. One way to achieve this can

be to have a robust trust center that can implement recommendations made in this paper. The paper will also identify the risks which cannot be mitigated completely so that the entities deploying ZigBee HANs understand them and account for them in their deployments.

The paper is focused on SEP 1.x specification used in HANs only. There are several other networks which are connected to the HAN like the neighborhood area network (NAN), backhaul network, and other non-ZigBee interfaces within a HAN. We will not specifically focus on these networks because they either do not use ZigBee technology or their architecture and security is not sufficiently detailed in the SEP 1.x specifications. While NAN is included in some of the discussions, we will not consider any specific NAN technology because current, and potentially future, deployments do not use ZigBee SEP 1.x profiles. The paper also identifies areas like NAN security as a network impacting the HAN security and will recommend to the applicable standards bodies to consider their architectures and security in detail in future versions of the specifications.

Finally, there are known issues regarding the licensing of the ZigBee specification with regard to making ZigBee implementations open source. This was because any implementer had to have a valid license for the intellectual property rights (IPR) and a valid license was granted only through membership. In the future, ZigBee SEP 2.0 will be open source.

# 2 Representative System Architectures

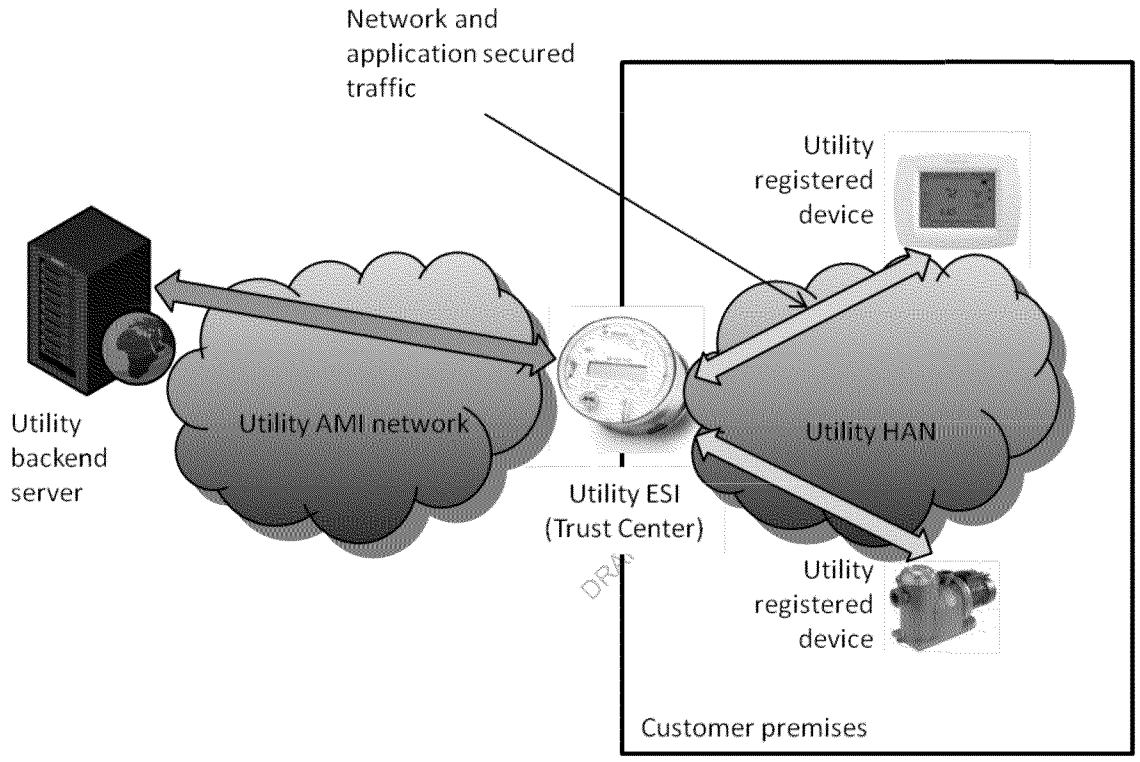


**Figure 1 - Utility Private HAN**

In Figure 1, all devices in the premises are managed by the utility and have to be registered with the Utility. There is one single HAN in the premises.

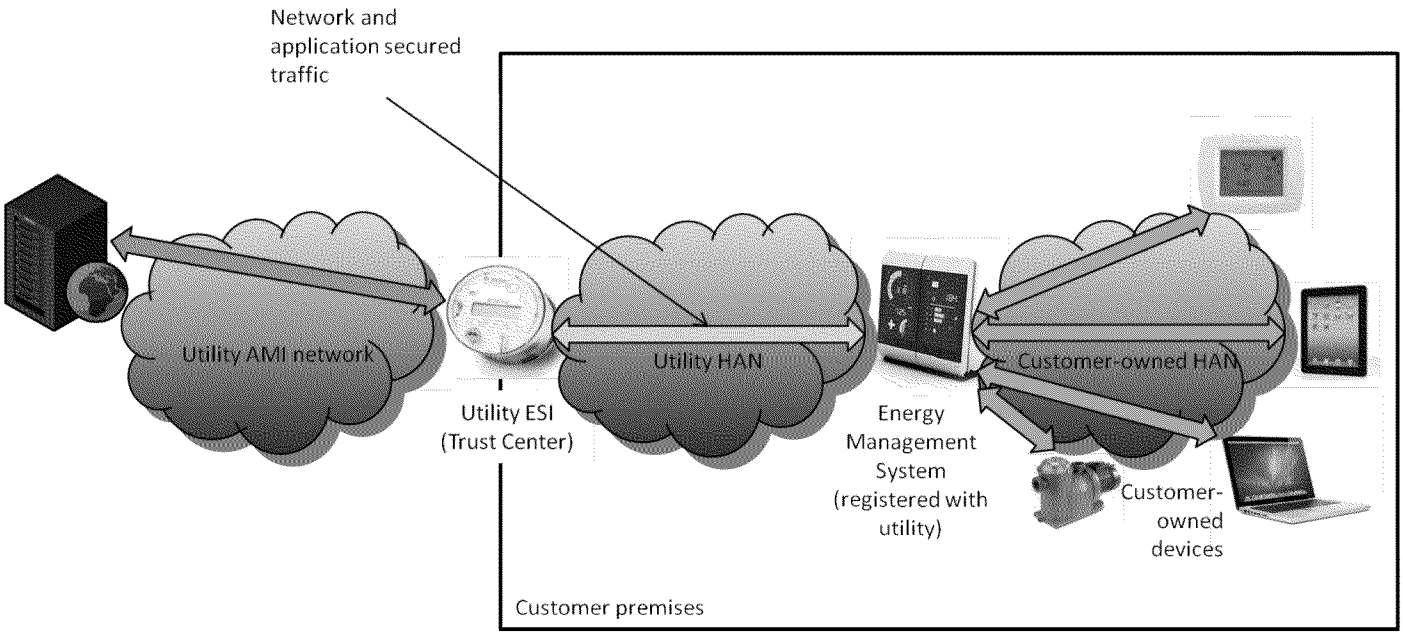


**Figure 2 - Customer Private HAN**

In the Figure 2, there is one device that has to be registered with the Utility. It is shown as an EMS in the figure, but may be a simpler device acting as an application layer gateway. This device has to be an SEP 1.x compliant device. There are two separate HANs in the premises. The devices on the customer-owned HAN do not have to be registered with the Utility and their functionality is independent of the SE 1.x specification. The coupling between the Utility HAN and the Customer-owned HAN depends on the functionality of the EMS/gateway.

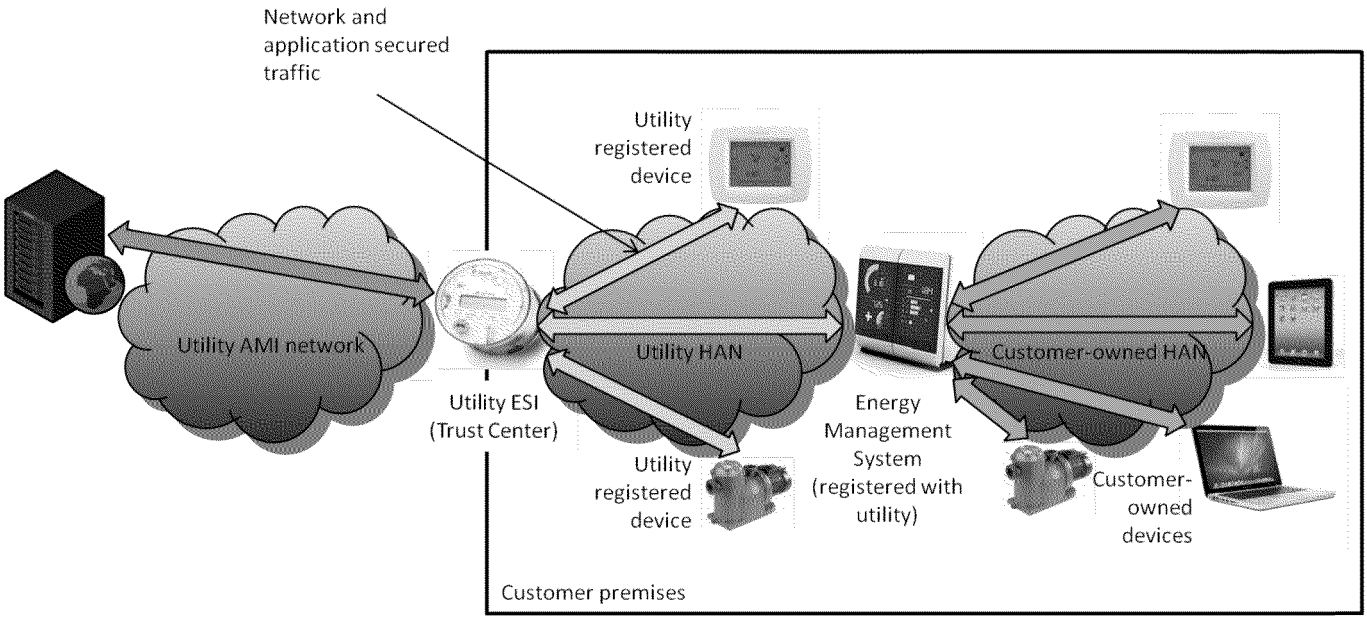


**Figure 3 - Utility and Customer Private HAN**

In Figure 3, some devices in the premises are solely managed by the utility and have to be registered with the Utility. An additional EMS is owned by the customer but has to be a SE 1.x compliant device and has to be registered with the Utility. There are two separate HANs in the premises. The devices on the customer-owned HAN do not have to be registered with the Utility and their functionality is independent of the SE 1.x specification. The coupling between the Utility HAN and the Customer-owned HAN depends on the functionality of the EMS.



## 2.1 Texas

A high-level discussion of the parties that interact in the DR system being implemented

in Texas. A draft illustration is included in Figure 4.

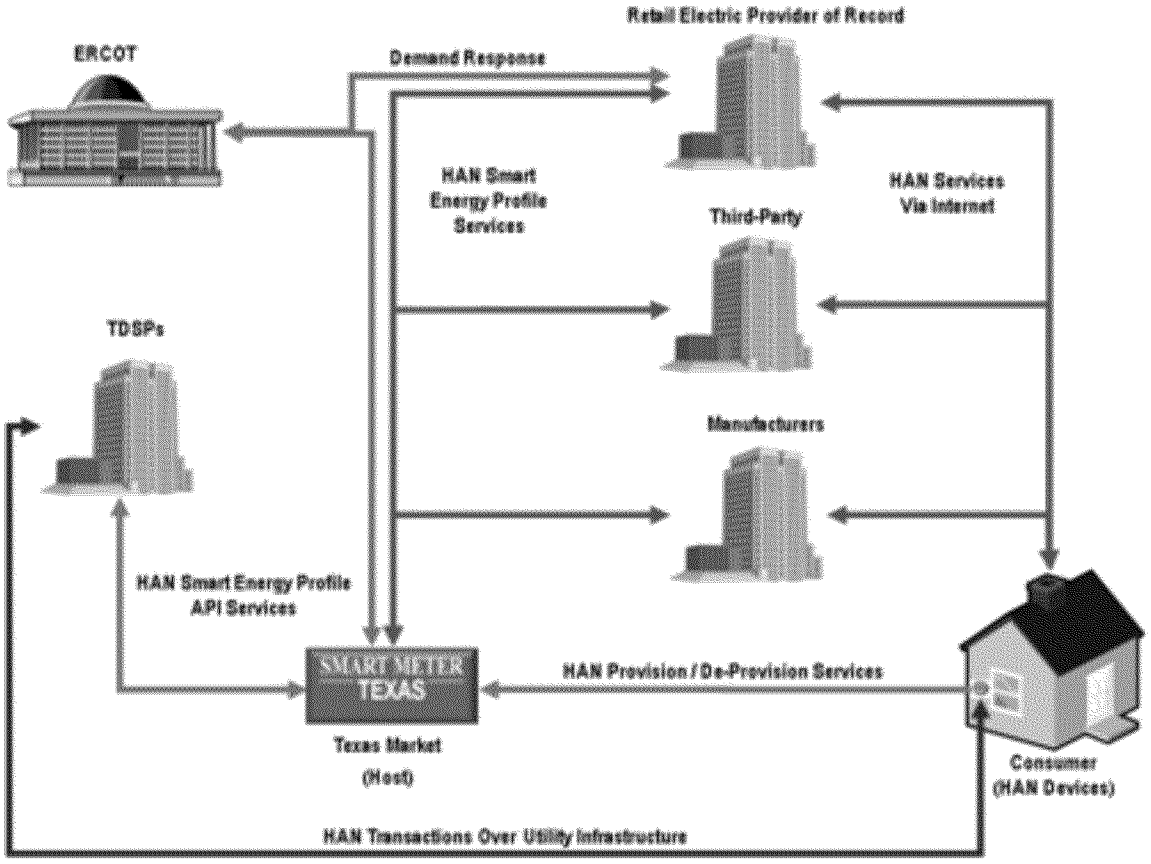


**Figure 4 - Texas Smart Grid Actors and Communication Paths**

A draft illustration of the communications pathway being implemented in Texas that enables the pricing information to be communicated to the Home Area Network is

included in Figure 5.

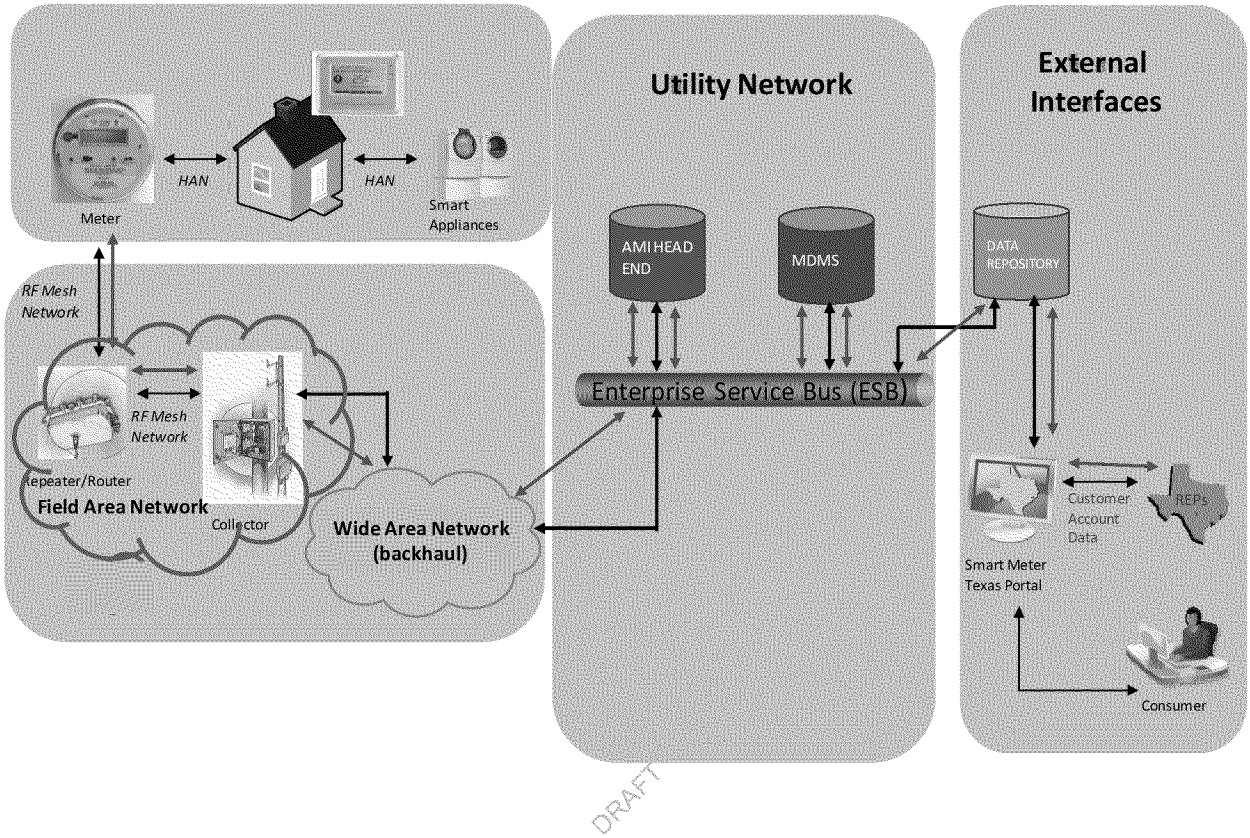


**Figure 5 - Texas HAN Communications Path and Interfaces**

(Note: There are many other communications networks in this diagram. It needs to be clear which are in scope for the analysis.)

Figure 6 shows an interconnection between the smart meter and the field area network (over the AMI). For this document, the AMI interface is outside scope. This analysis may consider the security of the AMI interface and the smart meter.

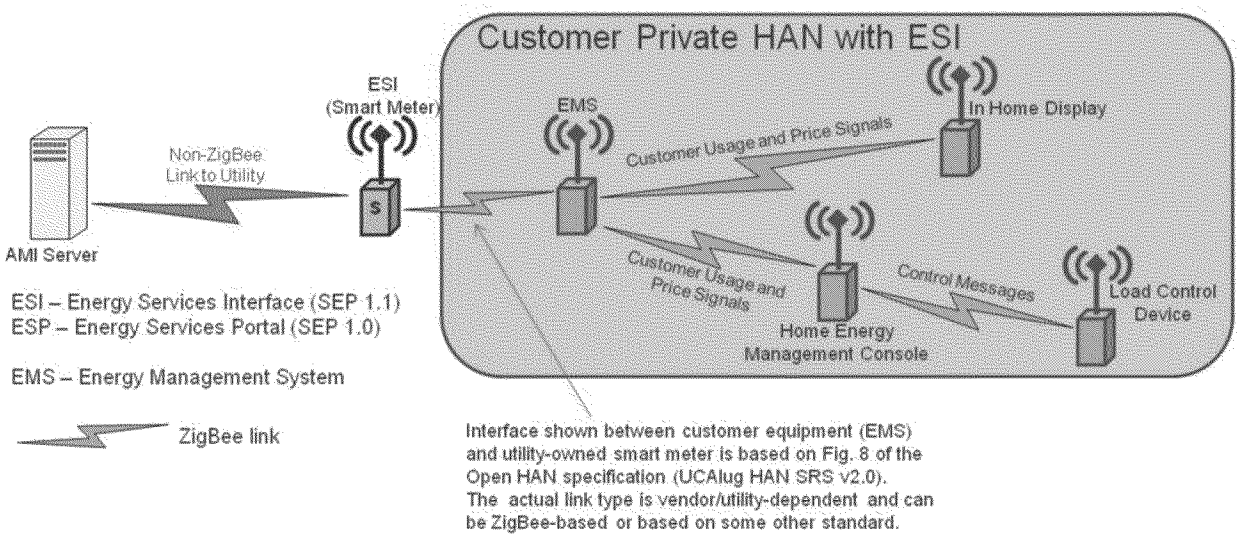


**Figure 6 - Customer Private HAN with ESI**[1]

## 2.2 California

A description and drawings of the architecture proposed in the Residential Energy Display Survey (REDS) project in California.



# 3 ZigBee SEP 1.x Overview

Included in this section is an overview of the security functionality specified for the ZigBee SEP 1.x.

# 4 NISTIR 7628 Security Requirements

The following security requirements from the NISTIR 7628 are applicable to the ZigBee SEP 1.x. Also included are

# 5 Potential Vulnerabilities, Impacts, Mitigations

This section includes the impacts and proposed mitigations to the identified potential vulnerabilities in the SEP 1.x specifications.

## 5.1 SEP 1.1 Cryptographic Specifications

One of the major components of SEP 1.x is cryptography that is used for authentication, integrity and confidentiality.

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

### 5.1.1 Key types: link keys, network keys, what other keys?

Uses Asymmetric (ECC) and Symmetric (AES)

ECMQV (80 bit) used for ECC public key exchange and key establishment for Link Keys (including those with the Trust Center):

There is only one network key for a HAN; all devices must have the network key to join the HAN. It is a symmetric shared key of AES-128-CCM*.

AES-CCM (128 bit) used with symmetric key for Network Key encryption/authentication and Link Key encryption/authentication

PRNG (deterministic): There is no specification, but there is a recommendation that the PRNG should conform to FIPS 140-2 (see 053474r18 (ZigBee Specification) Section 4.5.4.1). This is because there may be many suitable high entropy sources dependent on the hardware. (This needs clarification.)

The network key is generated by the Trust Center when the network is first started.

Look at table 5.13 for key types and usage in the SEP1.1 specification:

Key the stored (any security on it's storage?) in the coordinator and distributed to devices as they join the network

There are no particular recommendations on key storage due to the diversity of applications ZigBee is applied to. Again, an early vulnerability on an implementation whereby the AES key could be obtained using a syringe needle on an inter-chip communication line was demonstrated. Therefore, for certain device classes, it may be necessary to impose stricter requirements for key storage and protection. RCC

Install code is used to generate a key that secures the network key for transport to devices that are joining the network. How is this key generated?
DON: In document 075356r16 (the SE 1.1 Specification), Section 5.4.8.1.1 details how the Install Code is created. Also, Sections 5.4.8.1 and 5.4.1 detail how it is used for joining.

Key transport key is generated from the Trust Center using the MMO. Is the key transport key generated from the Install code?

DON: Correct, see the above cited sections of the SE 1.1 Specification.

The AES-MMO hash of the install code is used directly as an initial Trust Center link key, which is used to secure the transport of the network key. The install code itself is not secret as it is usually a manufacturer code printed on the device itself or its packaging. 075356r16 (SEP 1.1 specification) Section 5.4.8.1 gives details as a best practice. RCC

Only the trust center has knowledge of the install code and it is provided out-of-band to the trust center. The install code provides an authentication to the device that it has joined the proper network.

The utility headend must have the install code for specific devices added to the HAN and the device itself will also have its own install code.

The Trust Center will be configured with the install code out-of-band and performs the same AES-MMO operation to provide the shared initial Trust Center link key as the joining device. RCC

See section 5.4.5.4.1 of the core specification

Network key policy is not well defined for updates and modification, the same is true for the Link keys. Most deployments have static keys that are kept forever. (We need to make recommendations that keys need to be changed at regular intervals. We can reference the NIST SPs.)



Link Keys

Application Link key is based on the ECC (ECMQV)

Used for authentication of device

Used for generation of network key

It is not used for generation of network key. The CBKE-derived link key effectively replaces the initial TC link key based on the install code and is used as both an Application Link Key when communicating with the device which is also the TC, and as the TC Link Key. RCC

**Certicom is the only CA for this solution**

Revocation has never really been specified

Revocation is out of scope of HAN for SEP1.x but it is in 2.0 (Another point we want to make – that this is a potential vulnerability.

Revocation for millions of devices has real issues which need to be considered. It is optional in SE 2.0 and the aim is that it will be used for critical devices, e.g. EVs, DERs etc. RCC

Where is the trust center located? How is it setup and configured?

The coordinator that started the network, e.g., Utility Meter

Configuration and setup is not clear.

This is covered in ZigBee document 08-5195-02 (ZigBee PRO Trust Center Best Practices).

Link keys are a special key that is shared between a pair of communicating devices

Brokered through the Trust Center. More details on the brokering needed. DON: Details on how link key creation is brokered through the Trust Center can be found in 053474r18 Section 4.2.3.1 (Key Establishment) and 4.2.4 (Trust Center Role). A few things to remember reading these sections:

a. ZigBee SE 1.1 does not use SKKE (rather, it is allowing devices onto the network via the Install Code then asking the device to perform CBKE from the SE 1.1 Specification)
b. ZigBee SE 1.1 does not use High Security
c.

This is detailed in 075356r16 (SE 1.1 specification) Section 5.4.7.4 and the key transport mechanism is detailed in Section 4.4.3 of 053474r18. RCC

It is a symmetric key of AES-128

## 5.2 User interfaces, user interaction (security focused)

Nothing specified, out of scope.

## 5.3 Key establishment

Key generation

PRNG which is not specified??

DON: Correct the PRNG is not specified. The exact statements on PRNG are contained in 053474r18 Section 4.5.4.1.

The implication is the same random number requirements apply for the key establishment cluster as they do for all security services. This leads to 053474r18 (ZigBee Specification) Section 4.5.4.1 again. RCC

Key derivation

AES-MMO (MMO is not an approved mode – need to identify vulnerabilities.)
Insert reference here (p90 of SEP1.1 spec???)

### 5.3.1 Cryptographic algorithms

Cryptographic modes

CCM* This requires more details (Not on the FIPS approved list of modes. Need to identify potential vulnerabilities.)
DON: Reference is the IEEE 802.15.4-2006 specification, Annex B

RCC: 053474r18 (ZigBee Specification) Annex B.6

AES-CCM* when used in ENC-MIC mode is identical to AES-CCM, which is NIST-approved. ZigBee PRO always uses level 5, which is an ENC-MIC mode, therefore it is equivalent to AES-CCM. See 053474r18 (ZigBee Specification) Annex A and Annex B.1.2. RCC

Key sizes

128 bits for all AES



80bit ECC (ECMQV)

Key size is 163 bits in ECC, which is equivalent to 80 bits symmetrical. See NIST SP 800-57. RCC

### 5.3.2 Key management

Key usage, e.g., authentication, encryption, signing, integrity

AES-128-CCM* used for message integrity

AES-CCM provides confidentiality, message integrity and data origin authentication.
Signing using public keys is now optional as the CMU audit showed it has little use.
Public key cryptography is used for authentication and key agreement to provide symmetric link key. RCC

Need to fill in for encryption, signing, authentication…

Key storage

Are keys stored in protected memory, encrypted somehow, etc…????

There are no specific details in the specifications as they are primarily communication protocol specifications. There is some debate regarding further certification of more critical devices to include stricter requirements on physical security, storage etc. RCC

Key distribution

More details to be filled in, but some details in earlier parts of outline

Distribution of install code is important as it is used as the basis for a key transport key. RCC

HAN and NAN usage

NAN usage, none in the U.S. that we are currently aware of, but some may exist in other jurisdictions.

How do we address NAN as it is mentioned in the standard????? We can't simply say it is out of scope, but we could say that the current standard doesn't provide enough security definition to be used by a NAN.



### 5.3.3 Digital Certificates

Generation
Revocation
Usage

A more detailed description on the lifecycle of the certificate is definitely needed, including the arrangement with Certicom, delivery of certificates etc. RCC

### 5.3.4 Definition of the trust center

08-5195-02 (ZigBee PRO Trust Center Best Practices) gives more information here. RCC

### 5.3.5 Lifecycle activities: factory, device commissioning, etc. (device commissioning seems to be outside the scope???)

For each identified vulnerability also state potential impact and mitigations.

Ties in with certificate provisioning, install code generation etc. RCC

??

# 6 SEP 1.0 and SEP 1.1 Differences

The main changes are Trust Center swapout, which is not relevant to normal usage clarification on the install code and the addition of the OTA upgrade cluster, which has some security implications.

### 6.3.1 High level differences

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

2) Added text regarding Trust Center (TC) swapout procedures. This is fundamentally about how keys are stored and backed up and transferred. This is not certifiable text and stated as "subject to change"

   DON: We should comment on the security of the Trust Center swapout procedure. This was not addressed in the CSWG SE 1.0 and 1.1 review.

3) More prescriptive about post-joining procedure re. service discovery

4) Added text allowing TC to add and remove keys of device

5) Added text to explicitly discover the Key Establishment Cluster

6) Some tidying up of TC brokering of link keys

7) Clarification on install code format

8) Added formal procedure for joining, service discovery and device binding to tighten up interoperability

9) Added multiple ESI guidelines

10) Added OTA upgrade

DON: We should comment on the security of the OTA upgrade. This was not addressed in the SE 1.1 review.

11)Added tunnelling cluster

12)Tighter definition of Smart Energy device and concept of logical device

13)Many changes to metering cluster

14)Added mirroring to metering cluster

15)Many changes to price cluster

16)Added tunneling cluster

17)Added prepayment cluster (provisional)

DON: We should comment on prepayment since it was not addressed in the CSWG SE 1.1 review.

18)Added OTA cluster (separate document)

Focus on 1 – 8 for the discussion from a security standpoint.

## 6.4 SEP 1.1 general changes

The term ESP has been replaced by ESI

The term 'unsecured rejoin' is generally deprecated

OTA is added as a separate document

## 6.5 SEP 1.1 specific changes



5.2.1 Says that the TC and Coordinator shall be on the same node and it shall be *an* ESI as opposed to *the* ESI

Section 5.4.1: Language has been moved from 5.4.8.2.2 and thus made normative

Section 5.4.1.1 (Best practices' for tracking registered devices) moved from 5.4.8.2.1 and referred to directly

Section 5.4.2.2 adds text stating that text from 5.4.2.2.1 to 5.4.3 is provisional and not certifiable.

Section 5.4.2.2.1 (Initiating re-registration) moved from section 5.4.8.2.3.

Section 5.4.2.2.2 (Initiating de-registration) moved from section 5.4.8.2.4.

Section 5.4.2.2.3 is an added section for TC swapout. **This is a significant addition and should be carefully reviewed in line with policy and procedure.** This shows the limitation of an SE 1.1 network where there can only be one TC (although it does allude to multiple ESIs). The text is a little unclear in places – it talks about 'connect' to the new TC. Also requires upgrades to the device to perform the loss detection behavior. The idea is that it will detect some sort of failure on its existing network, then go off and look

for another network with the same ext. PAN ID. If it doesn't find one, it will go back to attempting to work on the existing network. It is expected all ZRs will perform this behavior periodically to determine if TC still exists.

DON: Trust Center swapout requires the backup of device credentials for all devices in the HAN and population of these credentials on the new Trust Center. Should evaluate the key material used for the backup and download of the HAN device credentials.

Section 5.4.3 adds some more text regarding making keys stale

Section 5.4.5 adds language describing processing after Joining and Key Establishment.

Section 5.4.7.2 adds text about multiple endpoints for Key Establishment cluster and that keys for specific can be added and removed but is outside of the scope of the specification.

Section 5.4.7.3 changes text to refer to the TC not as the ESI and add text about discovering the End Point where the Key Establishment cluster resides (possibly multiple). Interestingly, this now loses the association between the (an) ESI and the TC and therefore it is necessary to broker authorization to talk to the actual ESI if it is no longer the TC.



Section 5.4.7.4 removes text requiring that both nodes individually request the key.

Section 5.4.8.1 adds text about the randomness of the install code

Section 5.4.8.1.1.1 removes the source code for the CRC

Section 5.4.8.1.2.1 removes the source code for the MMO

Section 5.5.5 attempts to describe a more autonomous joining process and generally an attempt to improve interoperability by being more prescriptive about how devices should behave. **This is a significant addition and should be carefully reviewed.** This was absent in SE 1.0 (“It is expressly not allowed”). This is an attempt to mitigate at the flawed install code-based procedure.

Section 5.7 adds multi-ESI 'guidelines'. These are stated as provisional and not certifiable. **This is a significant addition and should be carefully reviewed.** Straight away this is flawed in that there is still only one TC. Who owns the TC? This would require some sort of brokering. Also requires concept of 'authoritative' ESI. This only makes sense when a single device is trying to arbitrate commands.

Section 6.1 states that manufacturers can add their own profiles.

Section 6.3 introduces idea of 'logical devices', i.e. a device within a device.

Annex B.7 is added – best practises for Inter-PAN

Annex C.3.1.1 adds text for discovery of Key Establishment cluster

Annex C.3.1.2.3.1.2 adds text for Key Establishment cluster stating that it should validate certificate out-of-band with its identity.

Annex E.2: Some clarifying text on overlapping issues

# 7 SEP 1.0 and SEP 1.1 implementation Guide

## 1.1. Implementation of CSWG Review Recommendations

Recommendations for how the potential vulnerabilities described in the Smart Energy Profile (SEP) 1.X reviews can be mitigated including information from the Texas and California projects.

#### *7.1.1.1 Trust Center*

#### *7.1.1.2 Certificate Revocation*

#### *7.1.1.3 HAN Network Key Handling*

#### *7.1.1.4 ECQV*

A discussion of the problems identified with the SEP ECQV requirements as related to NIST standards as well as the mitigation strategy used in current implementations (if applicable).

#### *7.1.1.5 AES-128-MMO*



#### *7.1.1.6 Key Management Policy*

#### *7.1.1.7 MAC Layer Security*

#### *7.1.1.8 Inter-PAN Capabilities*

#### *7.1.1.9 Boot-load Cluster Upgrade*

## 1.2. Assumptions

### 1.2.1. AMI/HAN Isolation

A brief description of larger overall system context within which HAN is implemented. Includes a description of expected and/or assumed levels of isolation between HAN and AMI networks and helps frame the utility and residential risk environment within which SEP 1.X security issues are being analyzed.

### 1.2.2. Utility HAN-focused Analysis

SEP 1.X security analysis that will focus on utility-centered HAN whose security policies and practices are approved by appropriate entities.

Includes discussion of customer HAN. However utility WAN, X10, other HAN protocols

are not in scope.

# 8 References


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 (This is the main application profile.)

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

4. NIST Special Publication (SP) 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004. Available from http://csrc.nist.gov

5. Federal Information Processing Standards Publication (FIPS) 197, Advanced Encryption Standard (AES), NIST, November 26, 2001, Available from http://csrc.nist.gov

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

7. Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, January 27, 2010 Version 2.0, www.secg.org

8. ECQV (80 bit) Implicit Certificates: Standards for Efficient Cryptography: SEC 4 (draft) ver 1.1r1: Elliptic Curve Cryptography, Certicom Research, June 9, 2006. Available from www.secg.org

9. California Public Utilities Commission, 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, July 29, 2011.

7. 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

8. 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

8. ZigBee SE 1.0 Security Analysis, Robert Cragie, date????

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

10. 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 (These are comments on a previous version of SEP 1.x. Some more background information.)

11. 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 (These are comments on a previous version of SEP 1.x. Some more background information.)

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

13. NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007, Available from http://csrc.nist.gov

14. NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004. Available from http://csrc.nist.gov

15. FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001. Available from http://csrc.nist.gov

16. FIPS Pub 198, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198, US Department of Commerce/N.I.S.T., Springfield, Virginia, March 6, 2002. Available from http://csrc.nist.gov

17. ZigBee 075390r04, ZigBee Alliance, ZigBee SE Profile: Protocol Implementation

Conformance (PICS) Proforma, December 2008. There are a variety of PICs documents referenced (Protocol Interchange Conformance statements). These documents describe what is mandatory and optional in a compliant implementation, for example:

a. MAC security - IEEE 802.15.4-2003 lists the feature as optional, the ZigBee 2007 Layer PICs and Stack Profiles 08006r03 lists the feature as excluded.
b. Standard Security vs. High Security - The ZigBee 2007 Layer PICs and Stack Profiles allow for either yet the ZigBee Smart Energy 1.1 PICs document prescribes Standard Security and precludes High Security Suggestion on PICs documents.

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

19. ZigBee Document 08006r03, ZigBee Alliance, ZigBee-2007 Layer PICS and Stack Profiles, Revision 03, June 2008 (The ZigBee 2007 Layer PICs and Stack Profiles - This document is the PICs (mandatory/optional items) that accompanies the ZigBee Specification (053474r18))

20. ZigBee Document 053474r18, ZigBee Alliance, ZigBee PRO Specification, June 18, 2009 (This document covers the stack below the application profile including network layer security and Trust Center policies. Here are a few relevant sections:
    i. Chapter 4 - Description of Security Services for both Application and Network Layers
    ii. Annex A and B - CCM* Mode of Operation and Security Building Blocks (Note: Standard Security (and not High Security) is used in ZigBee Smart Energy 1-1.) Symmetric Key - Key Establishment (SKKE), is not used in SEP 1.x
    iii. Chapter 2.4 - The Device Profile commands are available to devices which have not completed authentication and public key exchange
    iv. Chapter 3 - The Network Layer commands are available to devices that have not completed authentication and public key exchange.)
    v. ZigBee SEP 1.0/1.1 uses ZigBee PRO, which turns off MAC security (Network security is used as described in the ZigBee PRO Specification, 053474r18).

21. IEEE 802.15.4-2003 - This is a deprecated version of the IEEE 802.15.4 specification (current version is 2006)

22. ZigBee Document 095264r17, ZigBee Alliance, ZigBee Over-the-Air Upgrading Cluster, Version 0.7, March 14, 2010 (This document describes the capability added to SE 1.1 to perform over the air upgrade to devices in the HAN.)

23. ZigBee Document 095284r06, ZigBee Alliance, SEP 1.1 Over the Air Bootload Cluster PICs [protocol implementation conformance statement], 07 October 2010 (This document captures the mandatory/optional items for the Over the Air upgrade feature.)

24. ZigBee document 064309r04, ZigBee Alliance, Commissioning Framework.

Currently, there are no known SEP 1.x deployments using the Commissioning Framework. There are security issues associated with the Commissioning Framework, and additional cyber security analysis is needed related to SEP 1.x deployments.

25. 802.15.4-2003, IEEE Standard forInformation 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)