Key Management and Cryptography for Advanced Metering Infrastructures (AMI) and Other Large, Low Power Networks

Grant Gilchrist and Darren Highfill
EnerNex Corporation
170C Market Place Blvd. Knoxville TN 37922-2337
grant@enernex.com, darren@enernex.com

Abstract: Advanced Metering Infrastructures (AMI's) have limitations that require unique information security approaches. Some of the characteristics addressed in this paper include the mixture of one-way broadcast and two-way communication, the limited processing power found in organizational issues in managing cryptographic credentials, the sheer number of endpoints (in the millions), and the expected type and frequency of message traffic to be addressed.

This paper describes in detail the currently proposed authentication mechanism for broadcasting controls to Programmable Communicating Thermostats (PCT's) in the state of California. PCT's are a key component of the advanced metering and demand response infrastructure being deployed there. It discusses the alternatives that were considered in developing this mechanism.

This paper goes on to discuss some of the ideas currently under consideration for securing the two-way AMI networks, and how they might relate to this PCT solution.

Keywords: AMI, AMR, PCT

1 Introduction

The Programmable Communicating Thermostat (PCT) system is envisioned as a mechanism for reducing the amount of electrical power in use by the state of California during critical periods up to several hours in length. The intent of this system is to permit a statewide organization (as yet undefined) to send out a broadcast message that causes all thermostats in the state to automatically adjust themselves so the household uses less power. In this way the state can avoid blackouts or power system instability.

The broadcast message may be an emergency event, requesting an immediate curtailment of load, or it may be a price signal indicating that the cost of power will increase drastically. A price signal would permit some consumers to choose to continue using power at higher cost if they felt they could not curtail their power usage.

The state is in the process of mandating that all new homes built starting in 2009 will include a PCT. The legislation used to make this requirement is known as "Title 24" [1] [2]. This legislation will affect a fairly small number of homes relative to the size of the population, approximately 60,000 per year.

However, the investor-owned utilities (IOU's) in the state will also be deploying PCT's as part of Advanced Metering Infrastructure (AMI) programs affecting millions of homes per year. These thermostats will communicate with utilities through the home electrical meter, which will be connected to a wide-area network. These IOU AMI networks will vary depending on the utility and different geographic areas within the utilities' service areas.

The PCT's deployed by the utilities will be the same basic units as those installed as a part of the Title 24 program. The Title 24 legislation specifies a standard "expansion interface" on the PCT to accommodate the IOU network interface. When an IOU network interface card is installed in a thermostat, the Title 24 broadcast interface will be disabled.

The IOU metering networks will also require a security solution, but these will not be addressed by the Title 24 legislation. It would be helpful if the security solution for the broadcast Title 24 network shares components with that of the individual utilities' metering networks. Therefore, at least some of the security measures described in this paper are likely to be used in the two-way AMI networks.

2 Security Characteristics of the PCT System

There are a number of characteristics that make the PCT system unique from a security point of view [6]. However, it is interesting to note that many of them are common to utility networks other than metering. These characteristics are discussed in Table 1.

Characteristic	Description
Directionality	The messages for the Title 24 network will be one-way broadcasts or multicasts to the thermostats. The physical technology will be the US Radio Broadcast Data System (RBDS – NRSC-4-A) standard, which is currently used to provide information along with commercial FM radio broadcasts such as program names. This technology is also used by the state of California for the notification of statewide emergencies.
Processing Power	Current thermostats have limited processing power, often with only eight-bit processors and less than 1Mbyte of memory. Cost concerns make increasing processing power for PCT's unlikely in the short term. It is anticipated that the low-end "contractor" version of a PCT will retail for less than $50.
Number of Endpoints	The system must be able to secure millions of devices, representing millions of households. Some AMI networks currently being deployed must address between 3 to 5 million meters.
Addressing	It must be possible to send messages affecting only a specified subset of the thermostats.
Manufacturing	Thermostat vendors are prepared to modify their manufacturing processes to support key management for this system. However, it would understandably be preferable if the configuration of addressing and key material could be an easily automated process.

Characteristic	Description
Purchase	IOU's will purchase PCT's in bulk and distribute them when customers sign up for voluntary demand response programs. Building contractors will also purchase them in bulk. Eventually it is expected that customers will buy them at hardware stores.
Installation and Configuration	Thermostats must be installable by a construction contractor, a third-party installer hired by IOU's, or ideally, by a customer. Any installation procedures must therefore be extremely simple. A phone call to a 1-800 number, providing a serial number or key recorded on the thermostat, has been discussed.
Maintenance	After installation, any upgrade to security credentials, algorithms, or configuration must be performed remotely. The cost of traveling to a customer site is approximately the same as the cost of replacing the PCT.
Number of Messages	The number of messages transmitted is very small, perhaps three or four messages per day at maximum to any given thermostat. A "heartbeat" message is required so customers and installers can be sure that communications is established. A possible heartbeat period of 15 minutes has been discussed.
Types of Messages	Messages to be used on the broadcast network include: Clock Set (time, nextDST, DSToffset) Start Price Event (start time, stop time, ID, price) Emergency Event – Change Temperature (start time, stop time, ID, amount of change) Emergency Event – Set Temperature (start time, stop time, ID, absolute temperature) Cancel Event (ID) Other messages sent on the IOU networks may include "firmware download", "display message", or "voluntary event" commands.
Key Ownership and Operation	At the moment, the organization that will issue the broadcast messages has not been clearly identified. It could be the utilities, for instance, or the Independent System Operator (ISO), or even independent third parties. In any case, the physical issuing of the messages would be through a third-party RDBS system operator. The owner of the cryptographic keys to the system, has likewise not yet been identified. One must make the assumption that the System Owner and the System Operator are two different entities, and that there may be multiple System Operators who must be certified or approved by the System Owner.

Table 1 – PCT Security Characteristics

3 Some Possible Attack Scenarios

The working group in charge of developing the PCT security mechanism has identified the following scenarios for possible attacks or misuse at the application layer [3] [6]:

1. Attacker turns on all air-conditioning units, causing a sudden, excessive, unexpected load, possibly leading to blackouts or grid instability.
2. Attacker recalls an authentic emergency signal, preventing the required reduction in load and forcing utilities to take other measures such as blackouts or buying energy at higher costs.
3. Attacker shuts down all air conditioning units, causing annoyance and possible health concerns among some customers. Would be of more concern in states with more severe weather conditions.
4. Attacker downloads new software into the PCT or the PCT communications module. This attack will be nullified on the Title 24 PCT's by simply not acting on these types of messages if they come over the broadcast network.
5. Attacker sends false acknowledgements. Not an issue on the broadcast network.
6. Attacker issues false time synchronization, potentially causing events to occur sooner or later than they normally would have.
7. Attacker causes false messages to appear on the thermostat display, misleading customer and perhaps causing incorrect behavior that could affect load or cause overload of utility customer service, e.g. "Please call utility now."
8. A customer decreases the air conditioner setpoint prior to an expected event, or changes the time locally, causing air conditioning to run normally during the event.

The working group has identified the following scenarios for possible network or transport layer attacks:

1. Attacker takes control of head-end radio system through the initiating organization's internal network or its interfaces with third parties.
2. Attacker causes denial of service by flooding the head-end IP network with acknowledgements (from the two-way IOU networks) or other valid messages.
3. Attacker intercepts wireless messages.

The working group has identified the following physical layer attacks:

1. Attacker jams or sends false messages from a ground station or vehicle, affecting a limited number of thermostats
2. Attacker jams or sends false messages from a balloon or other aircraft, increasing range of the attack.
3. Customer disables thermostat antenna.

4 Issues for Cryptographic Measures

Given the attack scenarios discussed here, the working group identified a number of issues regarding the cryptographic portion of the security solution [6]. These issues and the decisions made by the group are described in Table 2.

Issue	Description	Decision
Confidentiality vs. Authentication	Is it necessary to keep the contents of the broadcast PCT messages secret, or is it sufficient to ensure they are authentic, from an authorized source, and have not been tampered with?	Only authentication and integrity checking is necessary.
Symmetric vs. Asymmetric Cryptography	Because the thermostat may pass through many hands: utility, manufacturer, installer, customer, etc., it seems likely that asymmetric keys would be very useful in this application. However, the amount of processing required is orders of magnitude higher, and the memory and code footprint required could raise costs considerably.	Use asymmetric cryptography because it is ideal for this application, but use a relatively low-impact set of algorithms, namely elliptic curves.
Authentication Methods	While encryption is not considered necessary for purposes of confidentiality, it was considered that it might require less processing power to encrypt the entire message as a form of authentication than to use another method of authentication and integrity checking, e.g. a cryptographic hash.	Use a digital signature rather than a simple cryptographic hash. This decision followed from the choice to use asymmetric keys.
Periodic Key Changing	Is has been suggested that there be multiple levels of keys, with the lowest level being symmetric and periodically changed using a higher level key to avoid eavesdropping attacks. Considering how infrequent the event messages are, however, it is not clear how often the keys would need to be changed.	Multiple levels of keys were chosen: a primary and a backup pair for the System Owner, and another pair for the System Operator. The use of symmetric session keys was not chosen since asymmetric cryptographic processing is necessary in any case and the messages will be infrequent.

Issue	Description	Decision
Number and Grouping of Keys	It was suggested that it would be preferable to have multiple sets of keys so that the number of customers affected by the compromise of any particular key or set of keys would be limited. It was suggested that key sets be randomly distributed among thermostats sold so that any attack could not be concentrated in a geographic area. Naturally, the more key groups there are, the more difficult it will be to manage the keys.	The solution chosen does not prevent the use of multiple sets of keys, but does not require it either.
Recovery from Key Compromise	An appropriate mechanism for recovering from the compromise of one or more keys is necessary. The method must not involve travel to the customer site. So far, the methods considered include using multiple levels of keys as discussed above, or using a finite number of keys preloaded in the thermostat.	The solution chosen will use three levels of keys: one for the System Operator and two for the System Owner. The Owner's keys will only be used at installation time or to revoke the current Operator's keys. If for some reason the Owner's primary key is compromised, a backup will be used.

Table 2 – Cryptographic Issues for the PCT Security Solution

5 PCT Security Solution

This section describes the security solution that was chosen for the PCT system. This solution required three different elements:

- Operational rules defined within the thermostats.
- Recommendations for system-level non-cryptographic measures like intrusion detection.
- Cryptographic measures to be taken on the broadcast channels.

The sub-sections which follow describe these three elements.

5.1 Operational Security Measures

The working group identified the following rules for the thermostat to reduce the vulnerability to attack [4]:

1. Thermostats shall not accept remote commands to increase energy usage except the cancel event message.

2. Thermostats shall have hard-coded limits on what setpoints will be accepted via remote commands, to prevent unsafe setpoints.
3. Thermostats shall randomly delay for up to 30 minutes after being instructed to normally end or cancel an energy reduction event, avoiding sudden increases in load on the grid. The display of the thermostat shall not indicate the end of the event until after the random delay.
4. Thermostats will never automatically increase energy usage at the end of an event by any more than they originally reduced it.
5. Time synchronization commands received via the remote network shall override any time set locally.

5.2 System Security Measures

The working group has no authority over the head end of the network, but can only define behavior for the thermostats themselves. However, it has identified the following recommended security measures for the network as a whole [4]:

1. Create an intrusion detection system for the broadcast network. Such a system might consist of receivers spaced over the service territory that can compare the received broadcast messages with what was actually transmitted, and thus identify a false transmitter.
2. Change the thermostat time frequently enough to reduce the effectiveness of time change attacks.
3. Use historical energy usage data from the metering system to detect when a customer has disabled the thermostat's antenna or is attempting to "game" the system.
4. Thermostats should include a non-modifiable, timestamped log of received messages. An example of such a mechanism would be a non-volatile memory card inserted in the expansion slot.

5.3 Cryptographic Security Measures

5.3.1 Digital Signatures

As discussed earlier, the primary security mechanism used on the broadcast channel will be the use of a digital signature on the broadcast messages [3]. The messages will be signed using a method consistent with the FIPS 186-2 Digital Signature Standard. The asymmetric cryptographic algorithm used will be the Elliptic Curve Digital Signature Algorithm (ECDSA) described in FIPS 186-2 and ANSI X9.62. The PCT must be capable of supporting a public key length of 256 bits or larger.

Each message will include a timestamp and other information to prevent replay attacks. It will compare received information with the most recent 512 messages and ignore duplicates.

Further details of the signature method (e.g. as elliptic curve family, key size, etc.) and other parameters necessary to ensure interoperability between the PCT and the statewide communication system are expected to be developed during 2008 and documented separately.

5.3.2 Key Installation

As discussed earlier, the most controversial issue in selecting this mechanism was the decision to use asymmetric cryptography, since it would have a large impact on the processing power required and therefore the cost of each thermostat. However, it was felt that the advantages of being able to safely distribute public keys via the broadcast network and not needing to manage secret symmetric keys during the manufacturing process greatly outweighed the processing power concerns.

One important issue for key management, however, was that the public keys cannot simply be built into the PCT at manufacturing time because the identity of the System Owner*,* the entity that would own the public keys, and the System Operator, that would send the messages, are not known at that time. For instance, the PCT may be shipped to one of several different regulatory or operational jurisdictions, each with a different Owner or Operator.

Given this restriction, the PCT key registration and activation sequence is illustrated in Figure 1 [4]. There are two objectives for this sequence:

1. The PCT must receive and authenticate the public keys for the system.
2. The System Operator must use the keys to activate the PCT.

The sequence begins when the Factory builds a unique, random, 160-bit number into each PCT. When the PCT is connected to the heating and cooling system on the customer premises, an Installer supplies this random number to the System Operator and thence to the System Owner. This step must be performed out-of-band for three reasons:

- The network is only one-way.
- The timing of the installation process and which PCT is being installed is important to authentication of the public keys.
- Unlike using a secret key, the System Owner and System Operator do not know all the random numbers issued to the PCT's.

This step could be performed by the Installer calling an automated phone system.

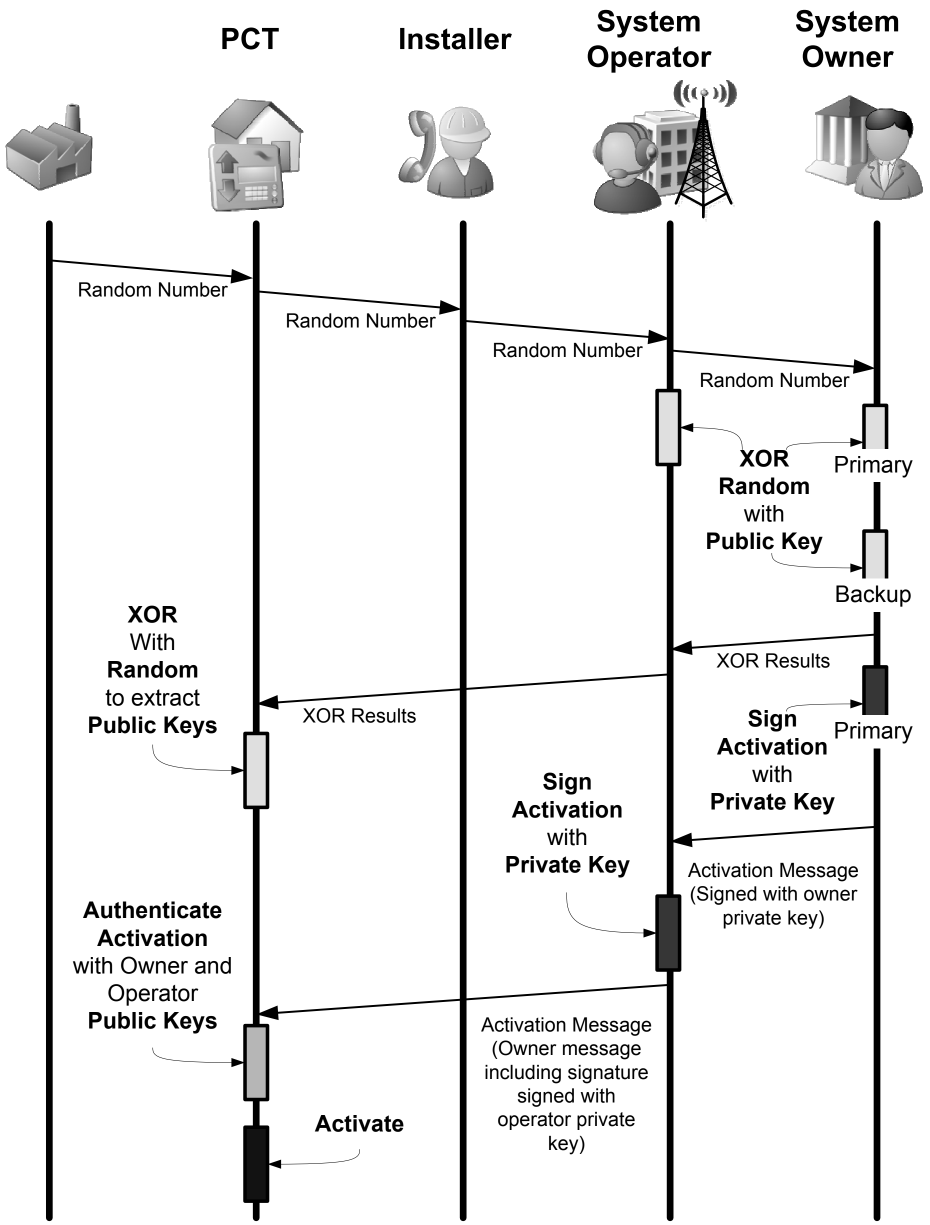
PCT
Installer
System Operator
System Owner
Random Number
Random Number
Random Number
Random Number
XOR Random with Public Key
Primary
Backup
XOR Results
XOR With Random to extract Public Keys
XOR Results
Sign Activation with Private Key
Primary
Sign Activation with Private Key
Activation Message (Signed with owner private key)
Authenticate Activation with Owner and Operator Public Keys
Activation Message (Owner message including signature signed with operator private key)
Activate

Figure 1 – PCT Registration and Activation Sequence

When the System Operator receives the PCT's random number, it broadcasts a message to *all* PCT's containing the System Operator's and System Owner's public keys combined with the new PCT's random number. In Figure 1, this combination process is shown as a simple XOR function, although in practice it could be something more complex.

When the PCT receives the registration message, it extracts the public keys by reversing the combination algorithm (e.g. XORing the message with its random number).

To complete the activation of the PCT, the Operator broadcasts a fixed, predefined activation message. All PCT's can hear the message, but only one will act on it. This message is signed twice: once by the System Operator to authenticate the activation and once by the System Owner, effectively authenticating both the activation and the System Operator's right to do so.

Following this activation step, the PCT will authenticate the signature on any broadcast message using the installed public keys.

5.3.3 Certification and Potential Attacks

The primary concern with the installation process described here is the possibility that an attacker may try to substitute a different set of public keys in place of the true keys, and thus gain control of the PCT. This is effectively an issue of certification: how can the PCT be sure that the set of public keys it has received are authentic?

However, a standard X.509 certificate cannot be used. Such a certificate would have to be signed by the System Owner, and as noted previously, both the System Operator and System Owner may not be known at manufacturing time. Therefore the public key needed to authenticate any certificate cannot be installed at that time.

The certification of the public keys is therefore achieved by a combination of the following elements:

- The **combination** of the random number with the public keys. Although the messages are broadcast, the key publishing and activation messages can only affect a single PCT at once; other PCT's will ignore it.

- The **random number** associated with each PCT. An attacker attempting to substitute a false set of public keys must know the random number associated with *each* PCT the attacker wishes to control. This is a barrier to the attacker, because as noted earlier in this paper, most of the useful attacks on the system require gaining control of a large number of PCT's.

  Even though there are millions of thermostats, the range of random numbers are 160-bits, so if the randomization function is well distributed, the range is therefore sparsely populated. So, attacking any given block of numbers is unlikely to have any useful effect for an attacker. An attacker would be unlikely to use a high-power transmitter for fear of being detected, and the probability of a significant number of PCT's both being found logically in a reasonably sized block of numbers *and* being found physically within range of a low-power transmitter becomes low in probability.

- The **out-of-band path** used to transmit the random number. Since the random number is never transmitted over the air, an attacker cannot learn it by eavesdropping. The physical address used to specify a particular PCT over the air is different from the random number.

- The **time of installation**. If the installation process is restricted by requiring the System Operator to transmit the public keys within a fixed time of receiving the random number, the probability of a successful attack is further reduced. This time restriction could be achieved by having the installer press a button on the thermostat before making the phone call.

With all these restrictions in place, an attacker would therefore need to:

- Know the valid random numbers for a significant set of PCT's.
- Be able to reach all the PCT's in that set with a transmitter, without being easily detected.
- Transmit the false keys within a small, fixed interval of each of the PCT's in the known set being installed.

An imposter installer or an authorized but disgruntled installer might be able to meet these requirements, if one had access to suitable equipment and knowledge. External processes could help mitigate this risk, such as vetting and authenticating all installers.

However, the best protection would be if the installation process was simple enough to be performed by the customer themselves. (This seems likely, since it would be comparable in complexity to the activation of a credit card.) If the customer was the installer, an attacker would then have no control over the time of the installation, and could not have physical access to the random number on the thermostat, short of following a particular thermostat home from the store.

Note that the cryptographic capabilities of the combination process (XOR in the example) are not vital to the certification of the keys. The combination function is not intended to keep the keys confidential, because the keys themselves are public and therefore not useful to an attacker. It is merely intended to reduce the number of PCT's that can be attacked during any particular registration process.

5.3.4 Key Revocation

The purpose of having three different public/private key pairs is to permit keys to be revoked and replaced. There are three possible scenarios:

- If the System Operator is replaced or the System Operator's private key is compromised, the new System Operator can publish their new public key in a message signed by the System Owner's primary private key.
- If the System Owner's primary private key is compromised, the System Owner can publish a new public key in a message signed with the System Owner's backup private key.
- If the System Owner's backup private key is compromised, all three public keys could be re-published by requesting customers to re-install their thermostats. This would be time-consuming and annoying to the customers, but would at least be possible without having to replace the thermostats. Care would have to

be taken that thermostats were not re-installed in large groups, or some of the attack scenarios discussed in the previous section would become more feasible.

6 Other Options Considered

There were at least three other options considered before adopting the key management mechanism discussed in this paper [5]:

- **Using Symmetric Shared Secret Keys.** This is an option used by some military systems, and is illustrated in Figure 2. Symmetric keys are used instead of using asymmetric keys. The manufacturer supplies the System Operator with half of a symmetric key and the corresponding serial number of the PCT. The manufacturer ships the thermostat with that half of the key installed.

  The other half of the secret key is chosen by the System Operator. When the Installer calls the System Operator, the Installer supplies the serial number of the PCT to be installed. The System Operator replies with the other half of the key. The Installer enters this number into the PCT. Now both the Operator and the PCT know both halves of the key, but the Manufacturer and the Installer do not. The Operator uses the two key halves to authenticate each subsequent broadcast message.

  This option was considered infeasible for several reasons:

  - It requires that both key halves inside the PCT remain physically secure, since these are symmetric keys. This cannot be guaranteed, especially considering the target cost of the PCT.

  - It requires a much more complex installation process, one involving entering numbers into the PCT and likely incurring more cost to provide such an interface. The process would also be twice as likely to be error-prone, since it not only requires human entry of the correct serial number but human entry of the correct second key half. If multiple levels of keys were added to permit key revocation, this concern would increase.

  - It requires both the Manufacturer and the Operator to maintain a list containing the serial numbers and key halves of all the PCTs. This is a security risk and additional cost and complexity.

  Some of these objections could be eliminated by using halves of an asymmetric public key instead of a symmetric key. However, it was pointed out that this would be needlessly complicating an asymmetric key system since the whole public key could be transmitted in the clear at any time. This led to the second option considered.

- **Installing the public keys at the factory.** This option is illustrated in Figure 3. As discussed previously, this option was considered infeasible because of the inability to know at manufacturing time the identity of the System Owner or the System Operator.

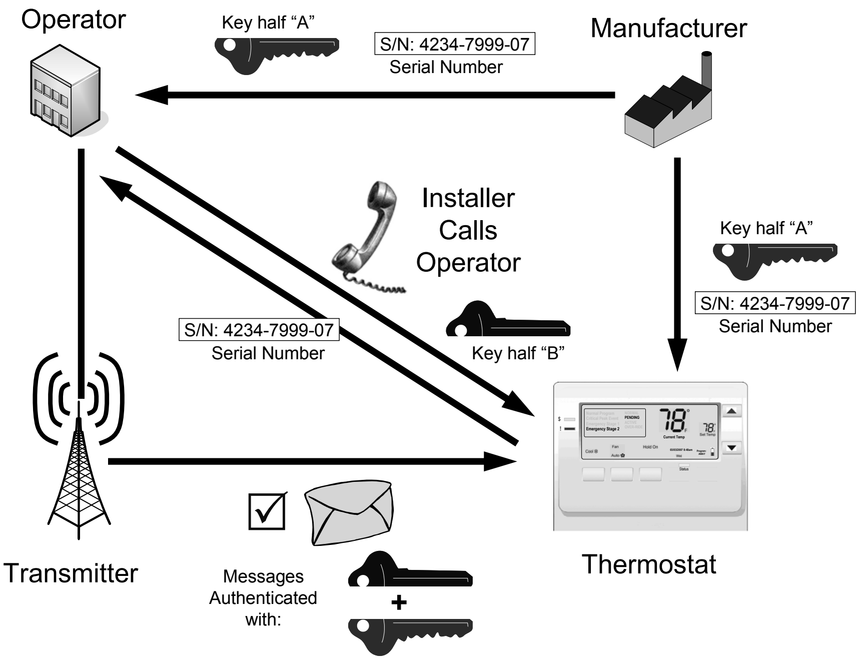

Figure 2 – Rejected Option: Symmetric Shared Secret Keys

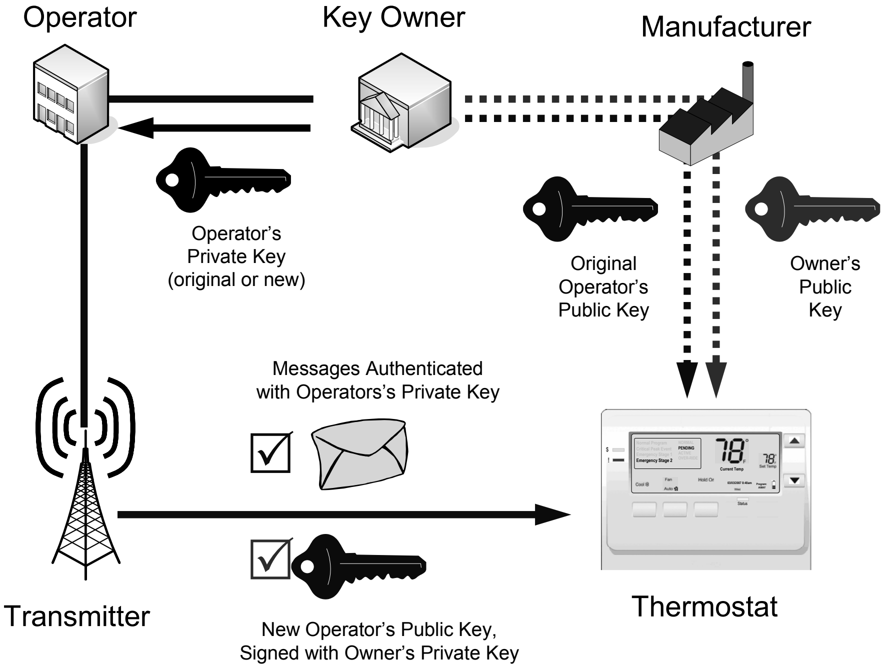

Figure 3 – Rejected Option: Installing Public Keys at the Factory

- **Using the TESLA protocol.** A body of work exists for performing broadcast authentication using symmetric keys, message authentication codes, and a protocol known as TESLA [9]. TESLA is based on the concept of a one-way chain of symmetric keys which are derived from each other and then revealed in reverse order. This option was considered infeasible for the following reasons:
    - TESLA requires a secure time synchronization mechanism, for which a digital signature based on asymmetric cryptography was proposed. It was felt that if digital signatures were required for the time synchronization mechanism anyway, they could be used for the primary security mechanism.
    - The mechanism for "seeding" the one-way chain at each end of the communications prior to installation would present the same concerns as the use of shared symmetric keys.
    - The one-way chain has a limited lifetime. At some point, the one-way chain must end and a new chain must be started. To "re-seed" the chain would require another level of keys and another security mechanism.

7 Ongoing Work on Two-Way AMI Security

This paper has described the solution chosen for the one-way broadcast demand response network being deployed in California. It is not clear at the time of writing how many elements of this system may be re-used in the two-way AMI and demand response systems that are to be deployed by the utilities. The development and standardization of that security system is being undertaken by the security working group of UtilityAMI, also known as AMI-SEC.

So far, the work is in the initial problem and requirements definition stages. The team has identified the service areas that it must secure, as illustrated in Figure 4 [8]. The functions listed around the edge of the circle represent only a small subset of the possible functions of an AMI that must be secured.

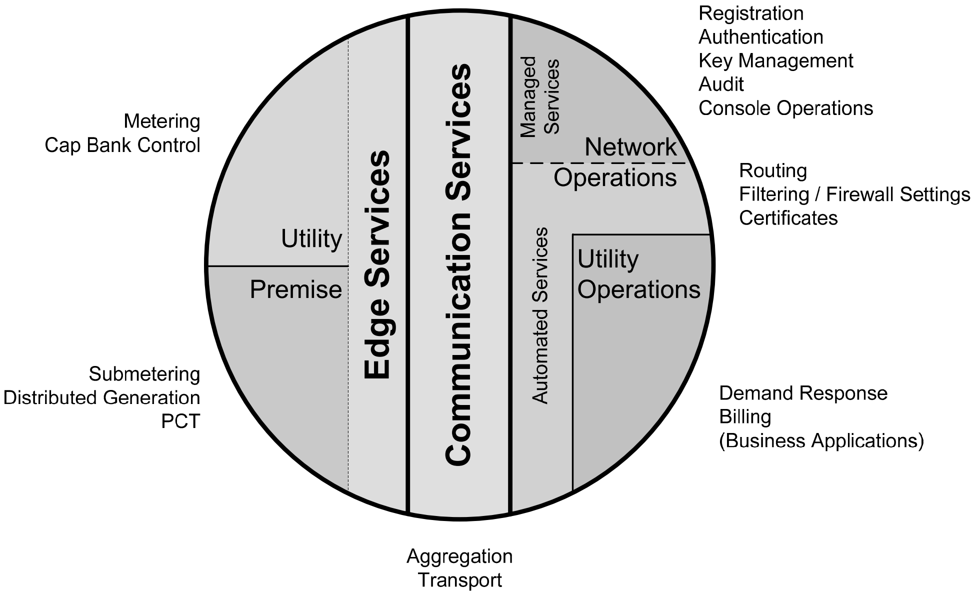

Figure 4 - AMI Service Areas to be Secured

The team has also identified a number of issues and questions that must be resolved [7]. Many of these resemble the characteristics of the one-way system that were discussed in Table 1:

- There is limited or no control over physical access to the devices.
- As shown in Figure 4, there are a wide range of types of logical access.
- There is a huge quantity of devices, numbering in the millions.
- The majority of the devices are resource-constrained.
- Data integrity and customer privacy must be protected.
- It is not clear how much intelligence should be required in the remote devices.
- Should the authentication mechanism be symmetric or asymmetric?
- Are measures like intrusion detection, tamper detection, and role-based access necessary?
- How to deal with the fact that networks and devices at the customer site may be purchased and owned by the customer?

However, it seems clear that there will also be a variety of issues and questions unique to a two-way AMI system.

Based on the services to be secured, UtilityAMI has also identified a number of AMI security domains, illustrated in Figure 5 [7]. This diagram illustrates the complexity of the standardization work. Each of the ovals represents a different set of security users, with different access requirements and rights. Each of the numbered circles represents a potential communications interface.

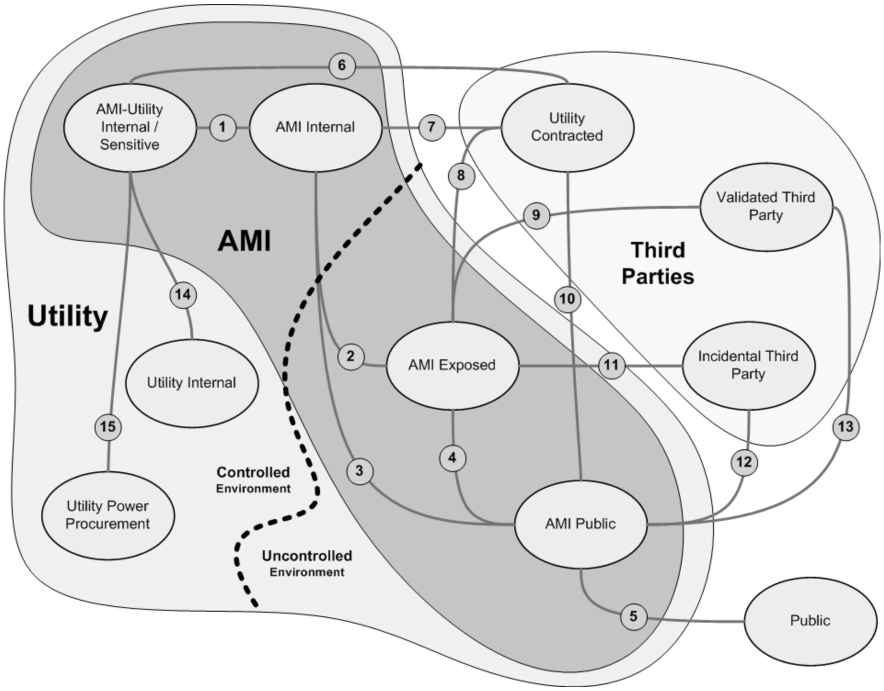

Figure 5 – UtilityAMI Domains and Interfaces

In addition to the work underway on securing the AMI system in general, there is specific work being undertaken by the OpenHAN working group. This group, also in accordance with UtilityAM, has the goal of securing the Home Area Networks (HAN's) which are likely to be used to connect customer equipment like PCT's to the two-way AMI network.

The following primary security issues recognized by the OpenHAN group are illustrated in Figure 6:

1. The HAN must be an open standard, and must be owned and operated by the customer, not the utility.
2. Nevertheless, several of the devices on the HAN, such as the PCT, appliances, air conditioning, pool pumps and perhaps even lights, must be controllable not only by the customer's home automation system, but by the utility AMI system – if authorized to do so.

3. The HAN may overlap with the HAN's of neighboring premises, but must not attempt to control or monitor the devices in the neighboring premises unless authorized to do so.
4. The utility's portion of the HAN may control and monitor multiple neighboring electric meters, and also certain gas or water meters, but again, only if authorized to do so.
5. All of these overlapping logical networks must be accessible via a common Advanced Metering Infrastructure and share a common physical media.

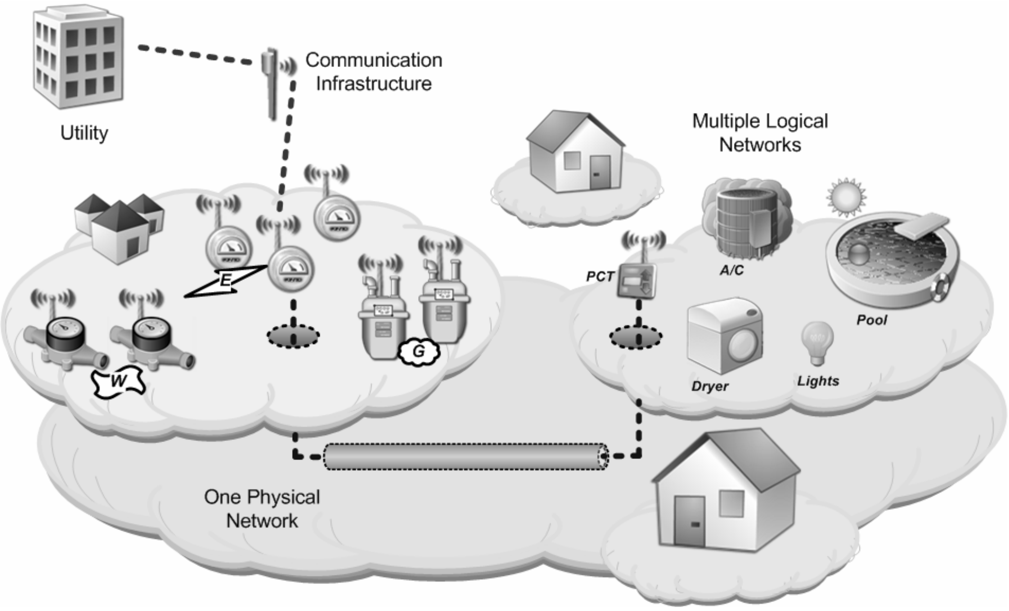

Figure 6 – Security Issues Surrounding Home Area Networks

8 Conclusion

The PCT security solution described in this paper has been released for comment and approval [1] [2]. While many details of its implementation remain to be resolved, the group of utilities, vendors, regulators and cryptographers who have helped to develop it are convinced that it will solve the problem of securing the one-way broadcast demand response network for California. As such it represents an important first step in securing the advanced metering and demand response infrastructures that will be deployed, and also a significant step toward securing the forthcoming "smart grid" that is currently a topic of much discussion in the industry.

Nevertheless, it is clear from the problem identification steps discussed in the second part of this paper [7] [8] that the PCT security solution was solved in a relatively short time because it addresses only a limited subset of the security concerns affecting AMI as a whole.

Not the least of these concerns is that the communications solutions currently being deployed for AMI are predominantly proprietary. The industry is still in the process of developing common object models, services, profiles, and network management mechanisms for AMI. Security solutions for AMI must be developed in parallel with these other communications standards.

This parallel development greatly increases the complexity of the problems to be solved. However, it must be considered encouraging that the need for AMI security has been clearly identified and that security requirements are being addressed so early in the process. This is the correct time to be doing so.

About the Authors – Grant Gilchrist, P. Eng., is a Consulting Engineer and Systems Architect on the Smart Grid Engineering Team at EnerNex Corporation. He is a member of several utility data communications standards bodies including the IEC working groups for SCADA, substation automation, protocol security, and interoperability. He is a founding member of the Technical Committee for the Distributed Network Protocol (DNP3). Most recently he has been active in the task force for an open Advanced Metering Infrastructure (OpenAMI), and is helping to develop the IEC 62351-5 standard for security of the IEC 60870-5 protocol family and their derivatives. He is a registered Professional Engineer in the province of Alberta, Canada.

Darren Highfill, CISSP, is a Utility Communications Security Architect and serves as the information security domain expert for EnerNex Corporation. He has been managing EnerNex's support of the Tennessee Valley Authority for several years and is one of the system architects for the PowerWAN – their new wide-area IP communications network. Darren has also been heavily involved in the integration of the Bradley County 500kV Substation: one of the first multi-relay vendor projects to implement the full suite of IEC 61850. He has also developed the information security framework that will be used to manage risk, write policy and produce specifications for Southern California Edison's AMI project and has adapted this framework for broader reference by the UtilityAMI forum. He is the co-chair of the AMI-SEC task force and co-wrote the security section of the California Energy Commission's Reference Design for Programmable Thermostats.

Acknowledgments – This paper includes quotations and summaries from the draft documents of the California demand response PCT working group and the UtilityAMI security working group. Please refer to the References.

References

[1] 2008 Building Efficiency Standards for Residential and Non-Residential Buildings – Express Terms, 45-day Language. (CEC-400-2007-017-45DAY). California Energy Commission, November 2007. http://www.energy.ca.gov/2007publications/CEC-400-2007-017/CEC-400-2007-017-45DAY.PDF

[2] Reference Appendices for the 2008 Building Efficiency Standards for Residential and Non-Residential Buildings – Express Terms, 45-day Language (CEC-400-2007-017-45DAY). Joint Appendix JA-5: Technical Specifications for Programmable Communicating Thermostats. California Energy Commission, November 2007. http://www.energy.ca.gov/2007publications/CEC-400-2007-020/CEC-400-2007-020-45DAY.PDF

[3] Reference Joint Appendix JA5: Technical Specifications for Programmable Communicating Thermostats Compliant with Title 24-200*8*. http://drrc.lbl.gov/pct/

[4] Reference Design For Programmable Communicating Thermostats Compliant with Title 24-2008. Editor: Erich Gunther. (Paper authors Grant Gilchrist and Darren Highfill contributors). March 2007. http://drrc.lbl.gov/pct/

[5] Possible PCT Key Structure. Presentation for PCT security working group, Grant Gilchrist, 2007

[6] Security Characteristics of the Title 24 PCT System. White paper for PCT security working group, Grant Gilchrist, 2007.

[7] Emerging Fronts: Advanced Metering and Interoperable Security. Presentation for AMI-SEC, Darren Highfill, 2007.

[8] AMI-SEC Working Group System Requirements Meeting. Presentation for AMI-SEC, Darren Highfill, 2007.

[9] The TESLA Broadcast Authentication Protocol. Perrig, Canneti, Tygar, Song. IEEE Crypto-bytes, 2002. http://www.cs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf