EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI)

1024431

Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI)

1024431

Technical Update, November 2012

EPRI Project Manager

A. Lee

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization prepared this report:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304-1338

Principal Investigator
A. Lee

This report describes research sponsored by EPRI. The material in this report is based on the work that was done by the Cyber Security Working Group (CSWG) Design Principles Group (DPG) under the Smart Grid Interoperability Panel. EPRI acknowledges the dedication and technical expertise of all the individuals who participate in the DPG.

This publication is a corporate document that should be cited in the literature in the following manner:

Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI). EPRI, Palo Alto, CA: 2012. 1024431.

ABSTRACT

Smart grid technologies are introducing millions of new intelligent components to the electric grid that communicate in much more advanced ways (two-way communications, dynamic optimization, and wired and wireless communications) than in the past. Cyber security is important because the bi-directional flow of two-way communication and control capabilities in the smart grid that will enable an array of new functionalities and applications.

One area of critical importance to the security of the modernized grid is cryptography. Cryptographic techniques are used to ensure confidentiality, non-repudiation, and authentication. In the advanced metering infrastructure (AMI) the smart meters include multiple symmetric and/or asymmetric key pairs. With the deployment of millions of smart meters, cryptographic key management for millions of keys is a critical technical area for utilities.

The overall objective of this research project was to identify the design principles that are applicable to AMI and the management of cryptographic keys. Designing and implementing effective cryptographic key management schemes is a research area that requires the input from utilities and the cryptography community.

This report may be used by utilities as they design their cryptographic key management systems and/or work with vendors to design cryptographic key management systems. The report provides specific design guidance for utilities.

Keywords
Cyber security
Cryptography
Cryptographic key management

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
BACKGROUND ON THE DESIGN PRINCIPLES GROUP (DPG)

The Cyber Security Working Group (CSWG) Design Principles Group (DPG) was founded to continue the work on bottom-up (BU) problems and design considerations developed by the BU and Cryptography subgroups that were included in the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security," August 2010. The DPG's focus is on creating a design principle's work product consisting of parts: design foundations, technical system design, and operational/organizational design. The intended consumers of the work product are asset owner organizations needing to procure secure[1] systems and devices, standards groups wanting to be better informed and aligned to unique smart grid security requirements, and system and device manufacturers that desire to increase the security of their solutions and be aligned to the NISTIR 7628 requirements.

The focus will be as technical and specific to real systems as possible while remaining agnostic to specific vendor solutions. As there are a wide range of systems, components, and operations to cover all of the Smart Grid domains, the work of the DPG may be divided into the following technical domains:

- Protection and control (P&C),
- Supervisory control and data acquisition (SCADA),
- Distribution automation (DA),
- Distributed Generation (DG),
- Demand Response (DR),
- Distribution Grid Management (DGM),
- Advanced metering infrastructure (AMI),
- Home Area Network (HAN),
- Electric vehicles (EV),
- Wide area monitoring, protection, and control (WAMPAC),
- Power plant industrial control systems (ICS), and
- IT support and management systems, network communications, etc.);

[1] In general the reference to "Secure" or "Trust" or "Trusted" is not meant to infer a definition equal to more formally defined systems or requirements as commonly found in federal standards and other certifications. These terms within the scope of the DPG, carry less formal but broadly understood industry definitions that are centered on making systems and devices more secure and trusted (as opposed to nothing being done, or the use of weaker, or misapplied stronger protection methods) based on known best practices and design approaches.

Potential operational domains are:

- Independent system operator (ISO),
- Transmission utility,
- Distribution utility,
- Co-operatives,
- Municipalities, and
- Outsourcers/cloud service providers, etc.).

There will also be cross-cutting security design foundations (e.g., cryptography and key management (C&KM), security event detection and response (SEDR), vulnerability management (VM), and trusted hardware/software (THS). Each of these crosscutting foundations will be represented in each technical domain, where relevant and unique needs must be specified. The DPG will examine, on a priority basis, the sequence in which these domains will be addressed. Similarly the operational domains will have representative elements of the technical domain where specialization of the technical design guidance is needed. Otherwise the operational domain will be focused on organizational and process factors.

The structure and process of the DPG is shown graphically in Figure 1-1 below:

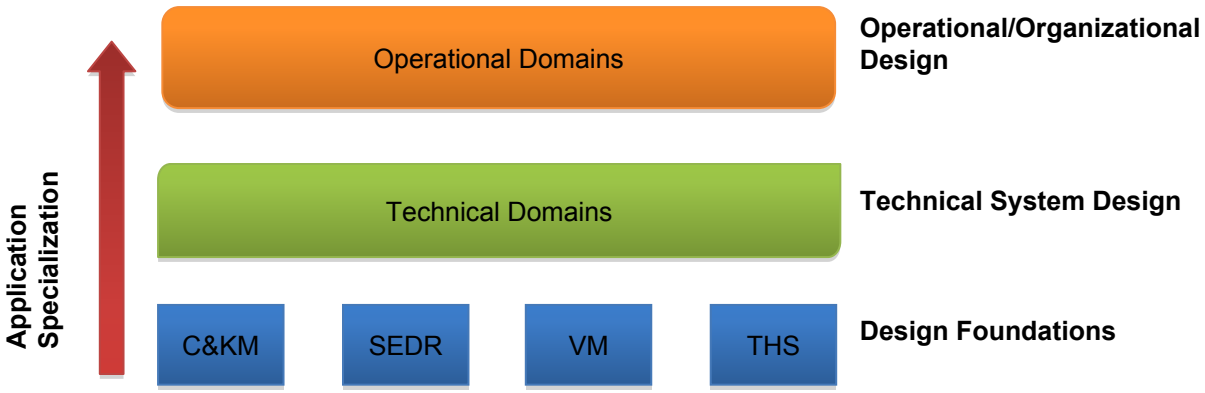

Figure 1-1
Structure and process of the DPG work

Each design principle will be specified using a template with the following sections:

1. Design principle class (Design Foundations, Technical Domain, Operational Domain)
2. General problem description (written and with optional diagrams and starting with the informative and then getting more technically detailed)
3. Affected domains (Technical and Operational)
4. General design considerations
5. Domain (Technical and Operational) Considerations
6. Applicable standards and best practices
7. Recommended enhancements to referenced standards and practices

8. Example technical problem solved using the design principle

The DPG initially focused on cryptographic key management and specifically on AMI. The National Electric Sector Cybersecurity Organization Resource (NESCOR) is a Department of Energy (DOE) funded public-private partnership that is led by EPRI. The DPG group was moved under NESCOR and continues to examine design principles. The first task of the DPG was to define design principles applicable to cryptography for the technical domains specified above.

2
CRYPTOGRAPHIC KEY MANAGEMENT SYSTEM (CKMS) OVERVIEW

The introductory material included in this section is intended to provide a high-level overview of a CKMS. The material is not intended to provide a comprehensive discussion of cryptography including cryptographic algorithms and cryptographic primitives.

Introduction[2]

Cryptography is often used to protect information from unauthorized disclosure, to detect unauthorized modification, and to authenticate the identities of system entities (e.g., individuals, organizations, devices or processes). Cryptography is particularly useful when data transmission or authentication occurs over communications networks where physical protection mechanisms are often cost-prohibitive or impossible to implement, as is typical in the electric sector. Cryptography can also provide a layer of protection against insiders and hackers who may have physical or possibly logical access to stored data, but not the authorization to know or modify the data (e.g., maintenance personnel or system users).

Cryptography can be used to provide three major types of data protection: confidentiality, integrity, and source authentication (also called non-repudiation).

a) *Confidentiality* protection safeguards data from unauthorized disclosure. Encryption algorithms are used to convert plaintext data into unintelligible ciphertext, while decryption algorithms are used to transform the ciphertext back to the original plaintext. The transformations are controlled by one or more cryptographic keys so that only the authorized parties who have the keys can successfully perform the transformations.

b) *Integrity* protection provides mechanisms to detect unauthorized data modifications. Cryptographic authentication algorithms typically calculate an authentication code or digital signature, which is a function of the data being protected and a cryptographic key used by the algorithm. It is highly unlikely that without possession of the correct key, an entity could modify the data and compute the correct authentication code or digital signature. Therefore, unauthorized modifications can be detected before the data is used.

c) *Source authentication/non-repudiation* provides assurance that the protected data came from an authorized entity. For example, a digital signature may be calculated on transmitted data. The receiver can verify the digital signature and therefore know that the data came from a particular entity.

---

[2] The introductory material was extracted from the National Institute of Standards and Technology (NIST) DRAFT Special Publication (SP) 800-130, A Framework for Designing Cryptographic Key Management Systems, April 2012.

There are two basic types of cryptography: symmetric and asymmetric. Typically, symmetric cryptography is used for confidentiality and both the sender and receiver use the same secret key. This is illustrated in Figure 2-1 below.

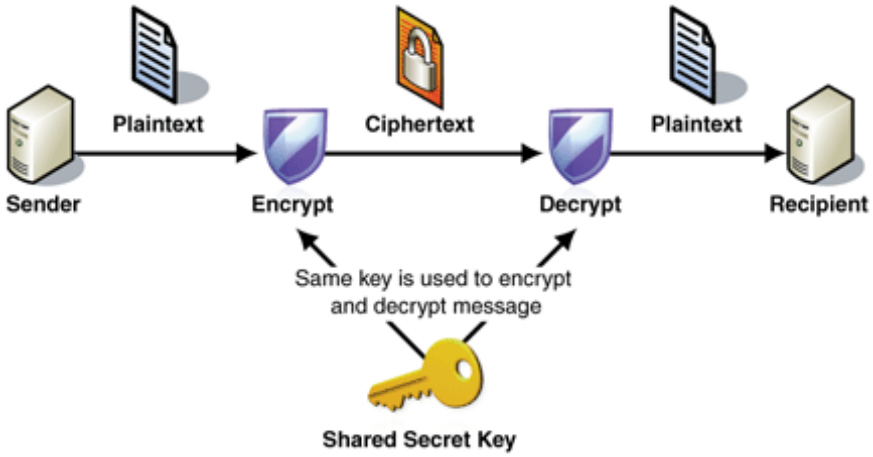

Figure 2-1
Symmetric Cryptography

Asymmetric cryptography is typically used for authenticity, non-repudiation, and integrity. In asymmetric cryptography, there are two related keys – a public key and a private key. The keys are mathematically related, but knowledge of one key does not give you knowledge of the other key. Figure 2-2 below provides a generic diagram of asymmetric cryptography.

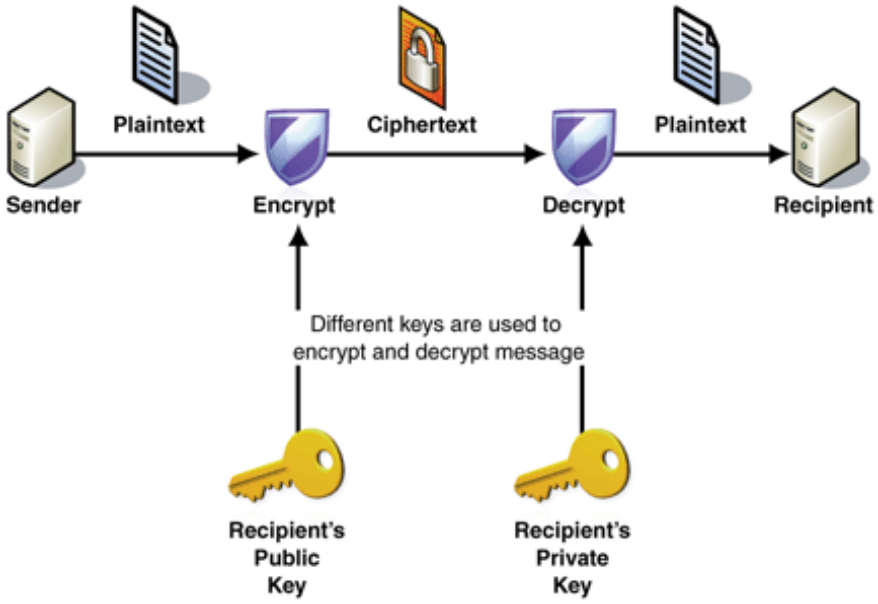

Figure 2-2
Asymmetric cryptography

Typically, in asymmetric cryptography, the message is sent in the clear to the recipient along with a digitally signed message digest. The recipient generates the same message digest, verifies the received digital signature, generates the message digest for the received message, and then

compares the two message digests. If they are the same, the data has not been altered in transmission. This process is illustrated in Figure 2-3 below.

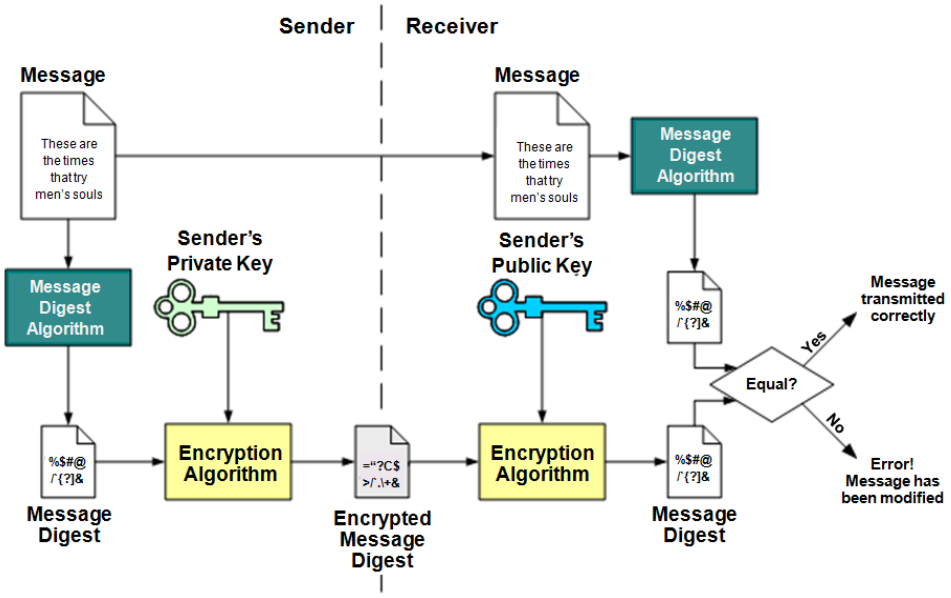

Figure 2-3
Digital Signature Generation and Verification

Cryptographic keys are managed and protected throughout their life cycles by a cryptographic key management system (CKMS). Cryptographic key management includes all the policies, procedures, and operations necessary to define, implement, and maintain cryptographic keys and associated data throughout the lifetime of the cryptographic keys. The lifecycle includes the following phases:

- Design
- Key Generation
- Key Storage
- Key Distribution
- Key Use
- Key Update
- Key Recovery
- Key Revocation/Suspension
- Key Backup
- Key Archive
- Key Destruction

A brief description of each phase is included below[3], with some issues that need to be addressed.

Design

Although a CKMS is typically smaller in scope than most IT systems, designing a CKMS will include all the elements required for the design of a secure system (e.g., data security, facility security, disaster recovery, etc.). Since cryptography is used to ensure the confidentiality, authenticity, and integrity of critical data, including commands and information, the design phase is critical.

Some of the design principles that need to be considered are:

- The use of cryptographic modules and the data that will be protected.
- Standards, protocols, regulations, and supporting services required for security interoperability.
- Security assessment, including self-testing, scalability testing, functional testing, environmental tests, and on-going assessments.

Key Generation

The life cycle begins with key generation. The steps used in the key generation process must always be secure against replication by potential attackers. Random numbers or pseudorandom numbers are frequently needed for cryptographic algorithms used in key generation and challenge/response protocols. Failure of an underlying random number generator can lead to the compromise of the cryptographic algorithm or protocol and therefore the device or system in which the weakness appears.

Many Smart Grid devices may have limited sources of entropy that can serve as good sources of true randomness. Design of a secure random number generator from limited entropy is extremely difficult. Thus it is particularly important that random number generation (RNG) design and implementation follow established approaches, and in some cases Smart Grid devices may need to include additional hardware to provide a good source for true bit randomization. Local key generation is not always possible due to end device limitations such as limited processor power, local memory constraints for storage and prime number computation, and limited storage space for the algorithms that generate these prime numbers.

Key Storage

After the cryptographic keys are generated, the keys must be stored and protected. Symmetric keys and private keys require confidentiality protection and access control. All keys require integrity protection. For confidentiality protection, cryptography, computer security, and/or physical security can be employed.

All stored keys require integrity protection because a garbled key will not correctly perform its intended function and may compromise another key under some circumstances. Physical security

---

[3] Several of the definitions were extracted from DRAFT NIST SP 800-130, A Framework for Designing Cryptographic Key Management Systems, April 2012.

may provide integrity protection for keys, but additional methods are frequently used.

Key Distribution

Cryptographic keys may be generated and used internally by a cryptographic module, distributed manually, or distributed electronically (typically called key transport). Some of the design decisions that need to be addressed are how keys are protected during transport, the key confirmation methods that are used, and the assurance methods used for identifiers in the key establishment methods.

Key Use

This defines how the various cryptographic keys are to be used, for example, encryption, authentication, digital signature, key transport, etc.

Some of the use considerations include:

- Who may use each cryptographic key, e.g., device type, device class, application, application class.
- The operations that may be performed, e.g., encrypt only, decrypt only, encrypt/decrypt, digital signature generation, digital signature verification, message authentication, integrity.
- The applicable organization security policies.

Key Update

This is the process used to replace a previously active key with a new key. This is important to ensure that keys do not remain in use too long. The organization needs to specify the cryptographic periods for the different keys.

Digital certificates contain public keys, cryptographic algorithms used, owner or subject data, the digital signature of a Certificate Authority that has verified the subject data, and a date range during which the certificate can be considered valid. Certificate lifetimes should be set to an amount of time commensurate with system risks and application; however as an upper bound it is recommended a maximum of 10 years not be surpassed. A more appropriate solution would be to determine reasonable lifetimes for each certificate. This is not a trivial issue, and different organizations may select different lifetimes for similar certificates.

Key Recovery

The process used to obtain or reconstruct a cryptographic key from backup or archive storage.

Key Revocation/Suspension

A previously active cryptographic key is no longer to be used to apply cryptographic protection to data. This is important if cryptographic keys become compromised. The organization needs to specify the circumstances under which a cryptographic key will be revoked or suspended, who is to be notified, and the information that is to be provided when the cryptographic key is revoked.

Key Backup

At least one copy of a key is placed in one or more secure storage facilities so that the

cryptographic key can be recovered if the original values are lost or modified during operational usage.

Key Archive

An electronic cryptographic key is placed into a long-term secure storage medium that will be maintained even if the storage technology changes.

Key Destruction

This is a key life cycle state in which a cryptographic key cannot be recovered or used. This occurs at the end of the cryptographic key life cycle.

CKMS Implementation Design Considerations

There are several design considerations that need to be addressed when implementing a CKMS. These are discussed below.

Public Key Infrastructure (PKI)

A public-key infrastructure (PKI) consists of protocols, services, and standards supporting applications of public-key cryptography. This may include a trust hierarchy based on public-key certificates, encryption and digital signature services provided to end-user applications, or services and protocols for managing public keys, often through the use of Certification Authority (CA) and Registration Authority (RA) components.

Among the services likely to be found in a PKI are the following:

- *Key registration*: issuing a new certificate for a public key.
- *Certificate revocation*: canceling a previously issued certificate.
- *Key selection*: obtaining a party's public key.
- *Trust evaluation*: determining whether a certificate is valid and the authorized operations.

Certificate provisioning involves several steps, including the:

1. Generation of a key pair with suitable entropy,
2. Generation of a certificate signing request (CSR) that is forwarded to a Registration Authority (RA) device,
3. Appropriate vetting of the CSR by the RA, and
4. Forwarding the CSR (signed by the RA) to the Certificate Authority (CA), which issues the certificate and stores it in a repository and/or sends it back to the subject (i.e., the device authorized to use the private key).

CAs need to be secured, RA operators need to be vetted, certificate revocation methods need to be maintained, certificate policies need to be defined, and so on.

The public key included in the CSR comes from a public/private key pair, which is generated specifically for use with the requested certificate. Access to the private key should be solely restricted to authorized parties. Ideally, the only party able to access the private key file is the subject that is represented in the certificate. The public key of the public/private key pair is required for the CSR, but the private key should never be sent to the CA under any circumstances.

3
AMI CKMS DESIGN CONSIDERATIONS

Smart meters that contain cryptographic keys for authentication, encryption, integrity, or other cryptographic operations require a cryptographic key management system (CKMS) that must provide for the adequate protection of cryptographic materials, as well as sufficient key diversity. That is, a smart meter, collector, or other power system device should not be subject to a break-once break-everywhere scenario, due to the use of one secret or private key or a common credential across the entire electric infrastructure. Each device should have unique credentials or key material such that compromise of one device does not impact other deployed devices. The CKMS must also support an appropriate lifecycle of periodic rekeying and revocation.

There are existing cases of large deployed meter bases using the same symmetric key across all meters - and even in different states. To share network services, adjacent utilities may even share and deploy that key information throughout both utility AMI networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

Also, some large deployed smart meter systems use a single asymmetric key pair to perform firmware updates. If the private key of the vendor (or utility) is compromised, all the smart meters may be compromised.

The ultimate decision on how to manage potential vulnerabilities, threats, and impacts must be based on a risk assessment that considers all factors in addition to the cyber security risks. This is particularly critical for a CKMS because cryptographic keys are used for security-relevant functions such as authentication, non-repudiation, encryption, and integrity verification. The following sections identify CKMS issues applicable to AMI.

AMI Architecture

Within a single utility, the overall AMI architecture may be considered a collection of cryptographic key management systems (CKMSs) because not every smart meter will be required to communicate with every other smart meter and the requirements for the individual CKMSs may be different. Many of these AMI subsystems will be of small to medium scale, particularly an AMI subsystem that includes smart meters that are configured in distinct mesh networks (or other configurations). At the highest level, the AMI architecture must be designed from two perspectives – (1) an overall large-scale system of systems that includes all of the individual AMI networks and (2) the individual AMI networks. The CKMS solutions for the two perspectives have different constraints and designing solutions for a large-scale deployment may over-constrain some of the potential solutions for the individual AMI networks.

The overall AMI architecture will also vary across organizations. Small municipalities and cooperatives may have only a few hundred or thousand customers, while large utilities may have several million customers. The CKMS for the different sized utilities may be different.

In addition, the CKMS needs to include the requirements for at least three different communities – vendors, the utility, and consumers. There are different requirements for each community, for example, roles and authorizations, certificate lifetime, and certificate revocation.

CKMS Operation in the Electric Sector

Security Staff: For the electric sector (including AMI), the CKMS systems will be extensively/primarily used by individuals who are not security experts and definitely not cryptography experts. In addition, the AMI systems and endpoints will typically be used by individuals with security as a secondary priority. As a result, the CKMS must function securely regardless of the user/administrator's security background and must not rely on complex and hard to apply policies and procedures that interfere with the primary utility mission of reliability.

Another aspect is that the pattern of interaction between users/administrators and devices in the electric sector will be radically different than the interaction in the typical IT enterprise. The electric sector users/administrators will need to operate remotely or locally and authenticate and authorize to multiple classes of devices and multiple devices within each class. For the smart grid, users/administrators must be able to access most devices remotely. Particularly for AMI, with thousands (and potentially millions) of smart meters, remote access is a requirement. Utilities (and vendors) need to have remote access to the smart meters for firmware upgrades, key replacement, etc. This is in contrast to *rolling* trucks to every smart meter to manually rekey millions of meters.

Local access to smart meters, when required by field personnel, may be performed through specialized input/output (I/O) devices such as optical port readers or front panel buttons rather than with a screen and keyboard. Field personnel may address specific technical problems, but they may also perform tests to determine if there are other technical problems with the smart meter.

All of these considerations must be included in the design of the CKMS and the different uses of the cryptographic keys, such as for authenticity, non-repudiation, confidentiality, and integrity.

Availability: In the electric sector, availability is the primary objective. This has specific implications for the implementation of the CKMS. For example, interruption of service due to cyber security events such as certificate expiration may be undesirable. Consequently, cryptographic key and digital certificate updating and migration must be considered to ensure that availability is maintained.

AMI Attributes

As described above, there will be hundreds of thousands of smart meters deployed across the country and cryptography is increasingly being used to address critical security requirements. With this large population of endpoints and the increased use of cryptography, automated cryptographic key management must be applied to a large set of devices and cryptographic keys – there may be several hundred million cryptographic keys. Manually managing all of these cryptographic keys is not an option.

Physical Environment: Smart grid equipment, such as smart meters, deployed in unprotected or lightly protected environments will, in some cases, process information and provide functionality that can be considered sensitive or valuable. In such cases, meters may include cryptographic

modules with a level of physical protection. When deploying smart grid equipment utilizing cryptographic modules, the environment, the value of the information, and the functionality protected by the module should be considered when assessing the level of physical protection required.

To address this physical access constraint, tamper response and/or tamper detection mechanisms for certain components may be required, such as for a cryptographic module. These tamper mechanisms may be in addition to those provided for the meter as a whole. However, in response to a tamper event, the sensitive information, including cryptographic keys, is commonly zeroized. This implementation approach is specified in Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. For the electric sector, this approach could result in communication (denial of service) and operational failures for the smart meters. Alternative approaches to tampering need to be developed. This is important because one design assumption for smart meters is that the tamper response/detection mechanisms will be defeated.

Some of the endpoints will be operational in challenging environmental conditions, such as heat, cold, dust, vibration, etc. These environmental conditions will need to be included in any tamper response/detection design and overly sensitive alarms must be avoided.

Life Span: The AMI equipment, including smart meters, has long life spans. Typically smart meters are expected to be operational for 15 years. This is in contrast to the lifespan for most IT and telecommunications equipment – which may be 6 months to 2 years. The smart meters must use cryptographic algorithms and cryptographic primitives that have long lifetimes. If the cryptographic algorithms are compromised because of new technologies or new cryptanalysis techniques, the CKMS and the smart meters must be upgradeable. This includes updating all the cryptographic keys.

The levels of confidentiality and value of the data or the operations will vary at different levels in the network. Key transport and re-keying (key update) need to be performed at intervals that are appropriate for the sensitivity of the data being protected (e.g., energy usage data) and the use of the keys (e.g., authentication). These update cycles need to be included in the CKMS design.

Communication Constraints: Many of the AMI endpoints will be communication bandwidth constrained. Consequently, long cryptographic keys, digital certificates, and lengthy negotiation sessions may not be appropriate for implementation in the smart meters. Also, endpoints may have sporadic connectivity or loss of communications for extended periods of time. The CKMS functions of key update, key revocation/suspension, and key distribution for potentially millions of cryptographic keys must be designed to ensure that all cryptographic keys are valid and critical operations are performed. Although smart meters are typically not considered critical power system devices – their use for other functions such as distributed automation and demand response is expanding. With these additional functions, ensuring the availability and validity of cryptographic algorithms and keys and digital certificates is more important. The availability requirement needs to be considered in designing the CKMS.

Processing Constraints: Computation and memory limitations are becoming less an issue in devices such as smart meters. However, some of the devices are battery operated and

cryptographic operations can significantly reduce the life of batteries. This is particularly an issue for public key cryptography and key generation.

PKI Issues and the Smart Grid: Standard PKI systems based on a peer-to-peer key establishment model where any peer may need to communicate with any other may not be necessary or desirable from a security standpoint for components in the smart grid. Many devices may not have connectivity to key servers, certificate authorities, Online Certificate Status Protocol (OCSP) servers, etc. Many connections between smart grid devices will have much longer durations (often permanent) than typical connections on the Internet.

In addition, operating a PKI for generating and handling certificates can also require a significant amount of overhead and is typically not appropriate for small and some midsized systems. A PKI-based solution, which can have a high cost of entry, but requires only one certificate per device (as opposed to one key per pair of communicating devices), and may be more appropriate for large systems, depending on the number of possible communicating pairs of devices.

Alternatively, small utilities could outsource their PKI. This is not necessarily the same as going to a public PKI provider, such as a large CA organization, and getting an "Internet model" certificate. With the Internet model, a certificate mainly proves that the individual is the rightful owner of the domain name listed in the certificate. For smart grid, this is probably not sufficient; certificates should be used to prove ownership, as well as provide authorization credentials.

The typical IT PKI does not meet the unique requirements of the electric sector. One research approach is to tailor the typical PKI model for AMI to address scalability. This AMI PKI would have autonomous zones and not a single/central point to manage all the various devices and would include both local and central authorities. This AMI PKI should process revocation in a more distributed and flexible manner, rather than using a centralized approach. A distributed/decentralized approach may be more applicable for the Certificate Revocation Lists (CRLs) as a single CRL can grow to an enormous size if devices are permitted to communicate with all devices, rather than a limited set of devices. The tradeoff is management of multiple CRLs.

Cryptography Design

Two areas specific to cryptography are critical for effective operation. The first is ensuring that the cryptographic key strength across the various algorithms is comparable and the second is deprecation of various cryptographic algorithms and key sizes. These are further defined below.

Cryptographic Key Strength: Cryptographic algorithms provide different "strengths" of security, depending on the algorithm and the key size used. Two algorithms are considered to be of comparable strength for the given key sizes (X and Y) if the amount of work needed to "break the algorithms" or determine the keys (with the given key sizes) is approximately the same using a given resource. The recommendations included in Appendix A (extracted from NIST SP 800-57, Part 1), are based on assessments made as of the publication of the SP using currently known methods. New or improved attacks or technologies may be developed that leave some of the current algorithms completely insecure.

Cryptographic key strength is applicable when implementing a CKMS. For example, if the symmetric key is an AES 128 bit key, the comparable elliptic curve cryptography (ECC) key size

is 256-383. This is critical when implementing key transport mechanisms; encrypting the symmetric key with an asymmetric key. If the key strengths are not comparable and the transport key (asymmetric) is less, the strength of the symmetric key is lessened. The guidance developed for the federal government was adopted by the CSWG and included in NISTIR 7628. This guidance has since been revised by NIST. The comparable key strength tables are included in Appendix A.

Cryptographic Deprecation: NIST has provided cryptographic key management guidance for many years. This guidance includes lessons learned over many years of addressing key management issues, and is intended to encourage the definition and implementation of appropriate key management procedures, to use algorithms that adequately protect sensitive information, and to plan ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. Based on the lessons learned, NIST has provided guidance on the time line for the deprecation of cryptographic algorithms and key sizes. Several of the deprecated cryptographic algorithms and key sizes are disallowed beyond 2013. Since many devices in the smart grid, including AMI and smart meters are intended to have a life time for 15 years or longer, utilities should work with the vendors and implementers to ensure that the appropriate cryptography is implemented. The deprecation tables are included in Appendix A.

4
CONCLUSION

With grid modernization, additional functionality is implemented in several domains, including the Advanced Metering Infrastructure (AMI). Cryptography is one of the security techniques being used to meet security requirements. Because of the scale of the AMI, potentially millions of endpoints will have cryptographic functionality. The CKMS to manage this significant design requires consideration of several design attributes and constraints. This technical updates provides an overview of CKMS, identifies differences with a typical IT/ telecommunication CKMS, and specifies CKMS design issues and considerations applicable to AMI.

5
REFERENCES

1. U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Length, January 2011. [government publication]
2. U.S. Department of Commerce, National Institute of Standards and Technology, DRAFT Special Publication 800-130, A Framework for Designing Cryptographic Key Management Systems, April 2012. [government publication]
3. U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-57, Part 1, Recommendation for Key Management: Part 1: General (Revision 3), July 2012.
4. U.S. Department of Commerce, National Institute of Standards and Technology, National Institute of Standards and Technology Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010. [government publication]
5. U.S. Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001. [government publication]

A
CRYPTOGRAPHIC TABLES

Included in this appendix are the comparable cryptographic key strength (from NIST SP 800-57, Part 1) and cryptographic algorithm and key deprecation tables extracted from NIST SP 800-131A.

Table A-1
Comparable Key Strengths (NIST SP 800-57)

Bits of Security	Symmetric Key Algorithms	FCC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

Table A-2
Hash Function Security Strengths (NIST SP 800-57)

Bits of Security	Digital Signatures and Hash-Only Applications	HMAC	Key Derivation Functions	Random Number Generation
80	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
112	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
128	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
192	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
256	SHA-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512

Table A-3
Asymetric Key – Approved Security Functions

Digital Signature Process	Use	
Digital Signature Generation	80 bits of security strength: DSA: ((|L| ≥ 1024) and (|N| ≥ 160)) and ((|*L*| < 2048) OR (|N| < 224)) RSA: 1024 ≤ |k| < 2048 EC: 160 ≤ |f| < 224	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	≥ 112 bits of security strength: DSA: |L| ≥ 2048 and |N| ≥ 224 RSA: |k| ≥ 2048 EC: |f| ≥ 224	Acceptable
Digital Signature Verification	80 bits of security strength: DSA: ((|L| ≥ 1024) and (|N| ≥ 160)) and ((|L| < 2048) OR (|N| < 224)) RSA: 1024 ≤ |k| < 2048 EC: 160 ≤ |f| < 224	Acceptable through 2010 Legacy-use after 2010
	≥ 112 bits of security strength: DSA: |L| ≥ 2048 and |N| ≥ 224 RSA: |k| ≥ 2048 EC: |f| ≥ 224	Acceptable

Table A-4
Hash Functions – Approved Security Functions

Hash Function	Use	
SHA-1	Digital signature generation	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	Digital signature verification	Acceptable through 2010 Legacy-use after 2010
	Non-digital signature generation applications	Acceptable
SHA-224	Acceptable for all hash function applications	
SHA-256		
SHA-384		
SHA-512		

Table A-5
Message Authentication – Approved Security Functions

MAC Algorithm	**Use**	
HMAC Generation	Key lengths ≥ 80 bits and < 112 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	Key lengths > 112	Acceptable
HMAC Verification	Key lengths ≥ 80 bits and < 112 bits	Acceptable through 2010 Legacy-use after 2010
	Key lengths ≥ 112 bits	Acceptable
CMAC Generation	Two-key Triple DES	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015
	AES and Three-key Triple DES	Acceptable
CMAC Verification	Two-key Triple DES	Acceptable through 2010 Legacy-use after 2010
	AES and Three-key Triple DES	Acceptable
CCM and GCM/GMAC Generation	AES	Acceptable
CCM and GCM/GMAC Verification	AES	Acceptable

Table A-6
Random Number Generation Transitions

Description	Use
RBGs specified in SP 800-90 (HASH, HMAC, CTR, DUAL_EC) and ANS X9.62-2005 (HMAC)	Acceptable
RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015
(Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	

Table A-7
Encryption Transitions

Algorithm	Use
Two-key Triple DES Encryption	Acceptable through 2010 Restricted use from 2011 through 2015 Disallowed after 2015
Two-key Triple DES Decryption	Acceptable through 2010 Legacy-use after 2010
Three-key Triple DES Encryption and Decryption	Acceptable
AES-128 Encryption and Decryption	Acceptable
AES-192 Encryption and Decryption	Acceptable
AES-256 Encryption and Decryption	Acceptable

Table A-8
Key Wrapping Techniques – Approved Security Functions

Algorithm	Use
Two-key Triple DES Key Wrap	Acceptable through 2010 Restricted use from 2011 through 2015 Disallowed after 2015
Two-key Triple DES Key Unwrap	Acceptable through 2010 Legacy-use after 2010
AES and Three-key Triple DES Key Wrap and Unwrap	Acceptable

Table A-9
Key Agreement (DH and MQV) – Approved Security Functions

Scheme	Use	
SP 800-56A and SP 800-135 DH and MQV schemes using finite fields	|p| = 1024 bits, and |q| = 160 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	|p| = 2048 bits, and |q| = 224 or 256 bits	Acceptable
SP 800-56A and SP 800-135 DH and MQV schemes using elliptic curves	160 ≤ |n| ≤ 223 bits and |h| ≤ 10	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	|n| ≥ 224 bits and *h* as specified in Table 9 below	Acceptable
Non-compliant DH and MQV schemes using finite fields	|p| ≥ 1024 bits, and |q| ≥ 160 bits	Acceptable through 2010 Deprecated from 2011 through 2013
	|p| ≥ 2048 bits, and |q| ≥ 224 bits	Deprecated after 2013. All other values of p and q are disallowed after 2013
Non-compliant DH and MQV schemes using elliptic curves	|n| ≥ 160	Acceptable through 2010 Deprecated from 2011 through 2013
	|n| ≥ 224	Deprecated after 2013. All other values of n are disallowed after 2013

Table A-10
EC Parameter Sets

	EB	EC	ED	ED
Length of *n*	224-255	256-383	384-511	512+
Maximum bit length of cofactor *h*	14	16	24	32

Table A-11
RSA-based Key Agreement and Key Transport Key Length Transitions

Scheme	Use	
SP 800-56B Key Agreement schemes	|n| = 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	|n| = 2048 bits	Acceptable
SP 800-56B Key Transport schemes	|n| = 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	|n| = 2048 bits	Acceptable
Non-56B-compliant Key Transport schemes	|n| = 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013
	|n| = 2048 bits	Deprecated after 2013 All other values of $n < 2048$ bits are disallowed after 2013

Table A-12
Key Length Transitions for a Key Derivation Function (KDF)

Algorithm	Use	
HMAC-based KDF	Acceptable	
CMAC-based KDF	Two-key TDES-based KDF	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015
	AES and Three-key Triple DES-based KDFs	Acceptable

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

1024431

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com