September 15, 2014

Cryptographic Key Management System (CKMS) for the United States Department of Energy (DOE) National Engineering Technology Laboratory (NETL)

- Final Report -

Prepared by:

Sypris Electronics, LLC
10901 N. McKinley Drive
Tampa, Florida 33612-6455

for the

U.S. Department of Energy
under contract
DE-OE0000543

Linked Table of Contents

Linked Table of Figures

1 List of Abbreviations

Abbreviation	Expansion
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
CA	Certificate Authority
CERIAS	Center for Education and Research in Information Assurance and Security
CKMS	Cryptographic Key Management System
CRADA	Collaborative Research and Development Agreement
CSEDS	Cyber Security for Energy Delivery Systems
CSES	Cyber Security Econometrics System
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOE-OE	Department of Energy Office of Electricity Delivery and Energy Reliability
EDS	Energy Delivery System
EPRI	Electric Power Research Institute
FIPS	Federal Information Processing Standards
HAN	Home Area Network
HSM	Hardware Security Module
IS	Information Security
ORNL	Oak Ridge National Laboratories
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition
SEIM	Security Event and Incident Management
XML	Extensible Markup Language

2 Abstract

This report summarizes the outcome of U.S. Department of Energy (DOE) contract DE-OE0000543, requesting the design of a Cryptographic Key Management System (CKMS) for the secure management of cryptographic keys for the energy sector infrastructure.

Prime contractor Sypris Electronics, in collaboration with Oak Ridge National Laboratories (ORNL), Electric Power Research Institute (EPRI), Valicore Technologies, and Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) and Smart Meter Integration Laboratory (SMIL), has designed, developed and evaluated the CKMS solution.

We provide an overview of the project in Section 3, review the core contributions of all contractors in Section 4, and discuss benefits to the DOE in Section 5. In Section 6 we describe the technical construction of the CKMS solution, and review its key contributions in Section 6.9. Section 7 describes the evaluation and demonstration of the CKMS solution in different environments. We summarize the key project objectives in Section 8, list publications resulting from the project in Section 9, and conclude with a discussion on commercialization in Section 10 and future work in Section 11.

3 Project Description

Sypris Electronics was awarded the U.S. Department of Energy (DOE) contract DE-OE0000543 to develop the Cryptographic Key Management System (CKMS) for the secure management of cryptographic keys for the energy sector infrastructure. The Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) Cyber Security for Energy Delivery Systems (CSEDS) industry-led program (DE-FOA-0000359), entitled "Innovation for Increasing Cyber Security for Energy Delivery Systems (I2CSEDS)", provides sponsorship for the development of Sypris Electronics CKMS solution.

The charter is to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks. The CSEDS program has found the critical energy infrastructures are vulnerable to cyber attacks, resulting in the potential for disruption of service and economic loss. The CKMS solution will primarily focus on the Advanced Metering Infrastructure (AMI) for the nation's developing smart grid infrastructure.

Sypris Electronics has sub-contracted Oak Ridge National Laboratories (ORNL) to provide technical support in assessing scientific and technological issues as they relate to the project. A Collaborative Research and Development Agreement (CRADA) was established (NFE-11-03562) to formalize the sub-contractor agreement between Sypris Electronics and ORNL.

The CKMS solution delivered by Sypris Electronics is tasked with protecting high value data in the energy sector infrastructure, following the best practices in cryptographic key management as established by the Department of Defense (DOD) to ensure a robust and secure solution. The CKMS solution was designed for handling command and control information, providing resilience against cyber attacks, and recovering quickly in the event of a cryptographic key compromise. To support these capabilities, the CKMS provides the secure generation, distribution, and revocation of cryptographic keys to the DOE smart grid infrastructure.

4 Project Team and Contributions

Team	Contribution
Sypris Electronics	Prime Contractor to the DOE, responsible for the design and implementation of the CKMS solution.
Purdue University CERIAS	Responsible for evaluating the security and robustness of the CKMS solution to potential cyber attack vectors.
Purdue University SMIL	Responsible for deploying a proof-of-concept CKMS solution on existing smart meter hardware and producing a demonstration of the CKMS capabilities.
ORNL	Responsible for testing and evaluating the key generation process, evaluating the security and usability of the proposed distribution methodology, and evaluating the key maintenance approaches for generation, distribution and revocation. These tasks were primarily accomplished through an application of the Cyber Security Econometrics System (CSES), which provides a qualitative assessment of risk to stakeholders in a system.
EPRI	Responsible for evaluating the CKMS solution from an industry perspective, which includes building a complete picture of the relevant components within the energy delivery network focusing associated with the Advanced Metering Infrastructure (AMI) and providing guidance for future CKMS research directions.
Valicore Technologies	Responsible for implementing core components of the CKMS solution leveraging their vCore Template Engine and Security Manager modules.

5 Project Benefits to DOE CSEDS

The DOE-OE CSEDS project has requested the support of industry, government, national laboratories and universities to advance and secure the critical energy infrastructure. The DOE-OE has found that the critical energy infrastructure, for example the AMI, is vulnerable to cyber attack vectors. In the event that the security of the critical energy infrastructure is compromised, large service disruptions, economic losses or potentially catastrophic loss of life may result. Thus, a critical objective of the DOE-OE has been to advance the security and robustness of the critical energy infrastructure.

The current project is supported by prime contractor Sypris Electronics, and sub-contractors ORNL, EPRI, Valicore Technologies and the CERIAS and SMIL groups from Purdue University. The development of the CKMS provides a solution for more robust and secure critical energy infrastructure, aiding in the mitigation of cyber attacks on control systems. This project specifically addresses Topic Area 2, "Centralized (Compartmentalized) Cryptographic Key Management" of the I2CSEDS project. The DOE and Department of Homeland Security (DHS) have outlined a broader Roadmap to Secure Control Systems in the Energy Sector, which plans to improve cyber security in the energy sector by collecting expert input from the control systems community.

Specific technical achievements from this project are outlined in this report with details related to the overall objectives captured in Section 9 (Summary of the Project Objectives).

6 Technical Discussion

6.1 Architecture

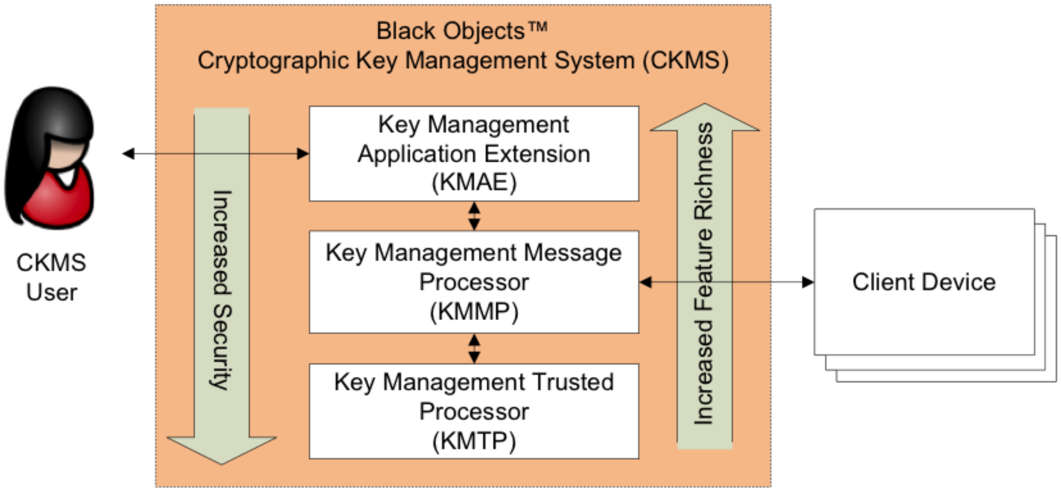

Black Objects™
Cryptographic Key Management System (CKMS)
CKMS User
Increased Security
Key Management Application Extension (KMAE)
Key Management Message Processor (KMMP)
Key Management Trusted Processor (KMTP)
Increased Feature Richness
Client Device

Figure 1: High Level Structure of the CKMS

The Cryptographic Key Management System (CKMS) is composed of three core components:

- **KMAE:** The Key Management Application Extension is a web application allowing an administrator or cryptographic key manager to interact with the CKMS and client protocol handlers.
- **KMMP:** The Key Management Message Processor provides secure message communication between client devices and applications. It uses template-based message processing for extending functionality in the future without requiring modifications to the underlying CKMS software.
- **KMTP:** The Key Management Trusted Processor is implemented as a hardware security module, providing access to critical key processing functions, including symmetric and asymmetric key generation, public key infrastructure (PKI) and certificate authority (CA).

Figure 1 illustrates the interaction of a CKMS user with a client device.

6.2 Software Stack

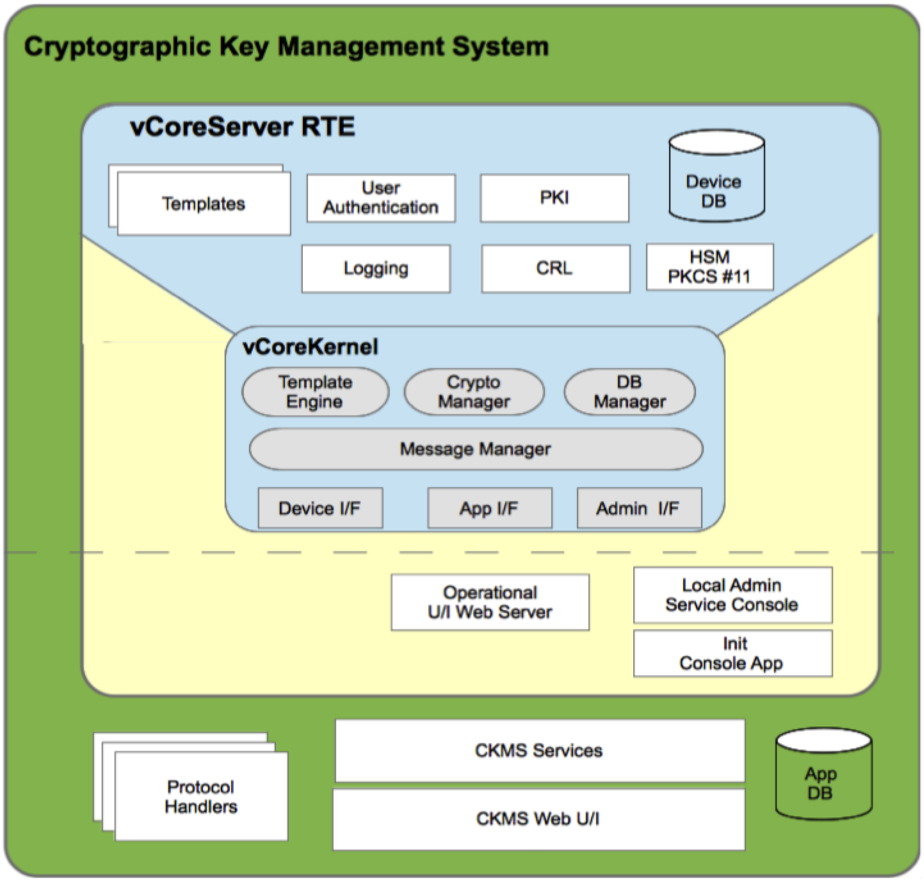


Figure 2: Software Stack of the CKMS

Figure 2 illustrates the software stack of the CKMS. The system employs FIPS 140-2 compliant cryptography, including the PKCS#11 cryptography interface and module for supporting key generation. This may be implemented in software libraries, or in the hardware security module (HSM). The system includes support for PKI X.509 certificates, as well as the generation and handling of PKCS#10 requests and usage in cryptographic signing operations.

The CKMS supports the authentication of users, such as administrators, security officers, and operators. Logging of events is accomplished through SYSLOG entries in a standard format to facilitate parsing and display to a user interface (UI) or external security event and incident management (SEIM).

Messages are based on an extensible markup language (XML) scheme, which facilitates future extensions to the CKMS without requiring modifications to the underlying software. The message templates enable communication between the user and Valicore Technologies' vCoreSecurity manager, which applies PKI operations (e.g., encryption, signatures).

6.3 Messaging Scenarios

Figure 3 illustrates the two messaging scenarios in the CKMS:

- **Scenario 1:** Both CKMS and the Utility connect to the Collector though the wide area network (WAN). CKMS distributes keys to the Utility as well as the end device. The security layer is required within the Utility for communication with the smart meter. This is beneficial if some of the messages between the Utility and smart meter don't require encryption.

- **Scenario 2:** This is essentially a "bump-in-the-stack" approach, where the Utility connects to the CKMS through the Application Interface. This allows the CKMS to authenticate and secure the communication link to the smart meter. The Utility is removed from cryptographic key management and the security layer.

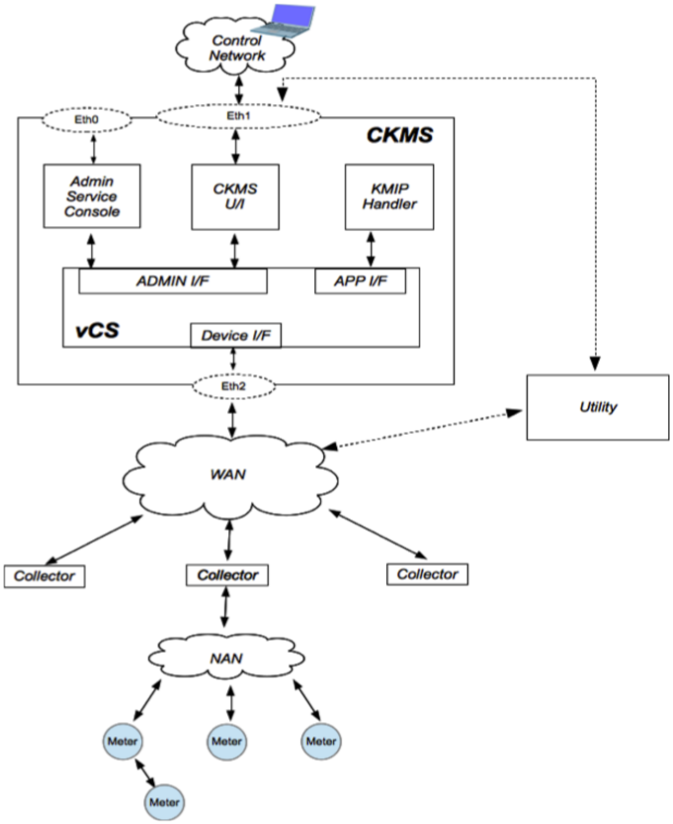


Figure 3: CKMS Messaging Scenarios

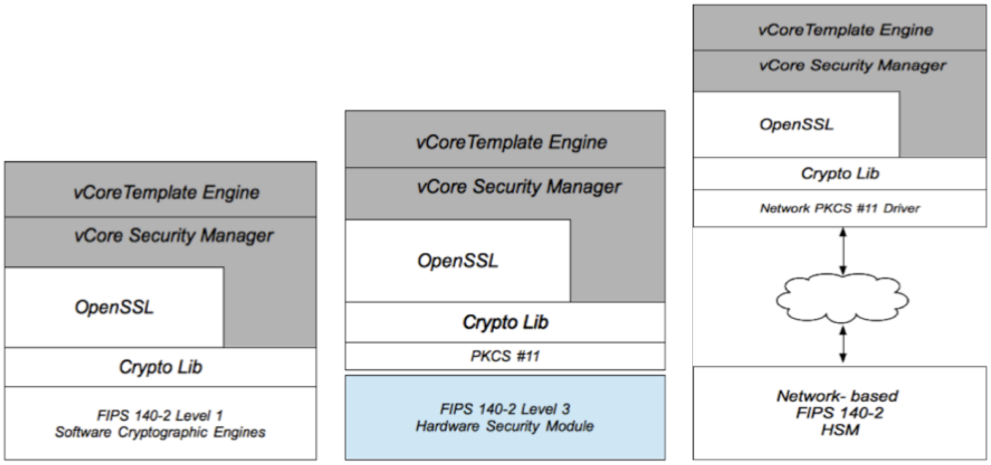


Figure 4: Security Module Options

6.4 Security Module Options

Depending on the deployment requirements, the CKMS supports three options for the integration of a security module. These options are illustrated in Figure 4 and described as follows:

- **Software-based Cryptography:** A software-based cryptography security module, where the cryptography library resides entirely in software. This option is most appropriate for product integration or for low cost deployments.

- **Embedded HSM:** A security module using an embedded hardware security module (HSM), where the cryptographic engine resides in a FIPS 140-2 Level 3 HSM. This option provides a small footprint for server installations but requires a server for each HSM.

- **Network HSM:** A networked HSM approach, where the cryptographic engine is external and connected via a network to the CKMS. This option allows for a sharing of a single HSM module across multiple servers.

A key attribute for all of the options is the common interface to the CKMS software application through the Crypto Library, allowing the transition from a software-based security module for initial testing to a hardware module for final deployment for stronger security.

6.5 Web User Interface

The CKMS Web-based User Interface (UI) allows end users to facilitate both device and key management. The current UI is for demonstration purposes only, and is not considered a final product. However, the application programming interface (API) supports more features than currently demonstrated in the UI, and may be extended based on the needs of the Utility.

The UI supports device management procedures, such as adding, deleting, viewing, importing and exporting devices in the CKMS. Example properties include the device ID, name, type, status and current key list. However, the XML format for device records allows additional properties to be added without modifying the underlying CKMS software.

The UI also supports key management procedures, such as modifying the properties of the key list (e.g., ID, name and type). As noted above, additional properties may be added to the key list structure without modifying the CKMS software due to the XML formatted records.

6.6 Scalability

Figure 5 illustrates the approach taken in the CKMS architecture to achieve a high degree of scalability. There are four key properties of the scalability design:

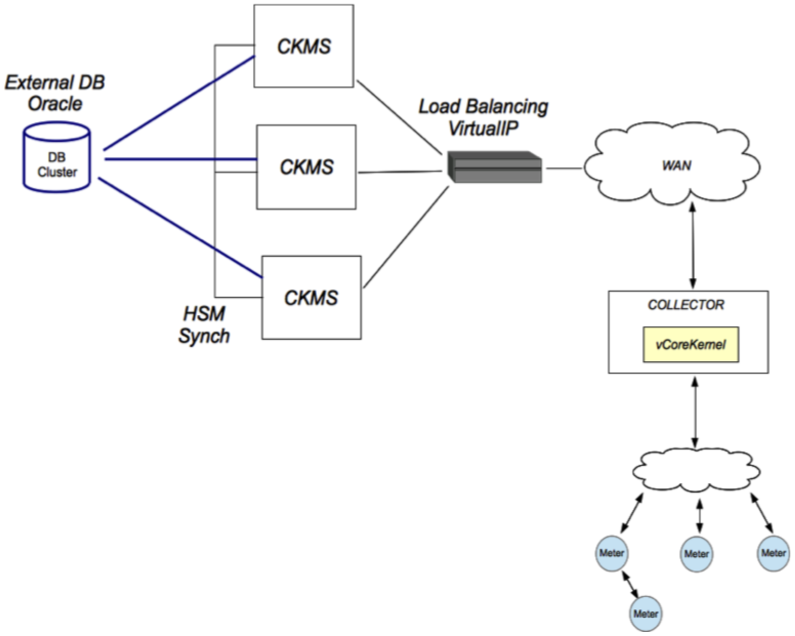


Figure 5: CKMS Scalability Approach

- **HSM Security Domain:** Responsible for enabling the distributed processing of keys across multiple servers to balance large loads.
- **Shared Storage of Wrapped Keys:** Enables the storage, access and manipulation of keys across multiple servers to balance large loads.
- **CKMS Database Replication:** Enables load balancing of user sessions across multiple servers to support a large user base.
- **Load Balancing Virtual IP:** Enables dynamic routing of messages across CKMS servers based on current load.

6.7 Purdue University Smart Meter Testbed

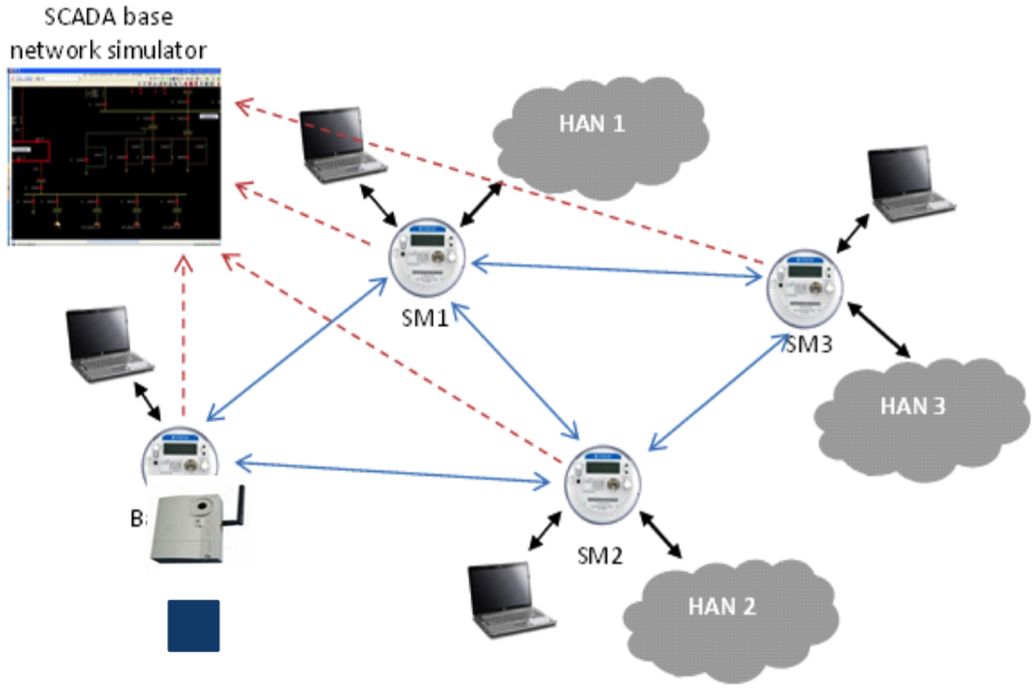


Figure 6: Purdue SMIL Testbed Structure of the CKMS

The Purdue University SMIL testbed included a small number of physical Landis+Gyr metering boards interfacing with a custom communication board implementing the CKMS key management protocols. These smart meters were connected to the CKMS in a laboratory environment with additional options for simulating a SCADA network. The testbed allows for detailed data captures of the message exchanges between all smart meter nodes within the network.

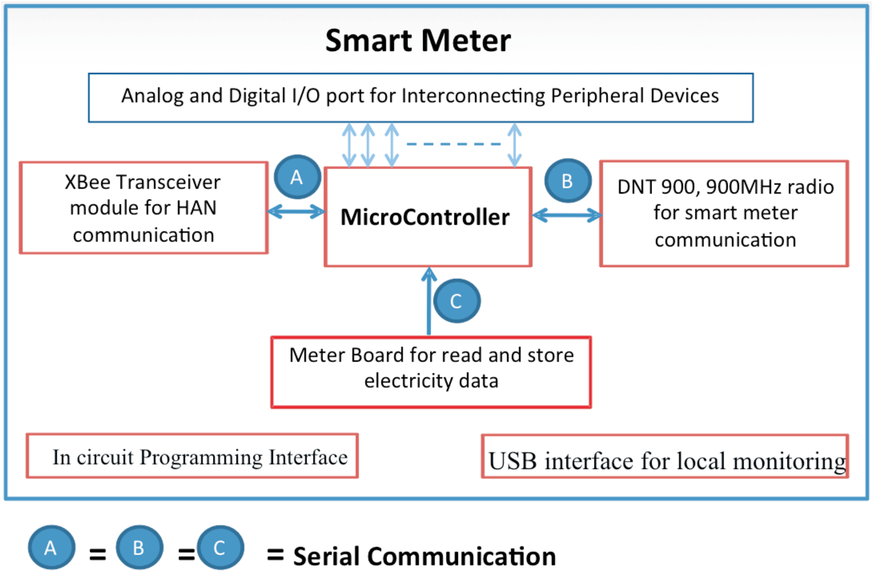

Smart Meter
Analog and Digital I/O port for Interconnecting Peripheral Devices
XBee Transceiver module for HAN communication
A
MicroController
B
DNT 900, 900MHz radio for smart meter communication
C
Meter Board for read and store electricity data
In circuit Programming Interface
USB interface for local monitoring
A = B = C = Serial Communication

Figure 7: Purdue SMIL Smart Meter Structure

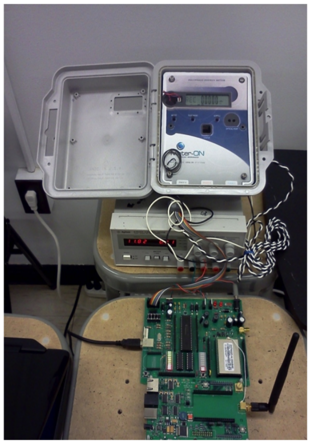


Figure 8: Smart Meter

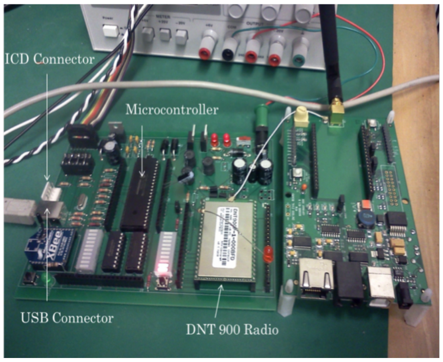


Figure 9: Communication Board

Figure 7 illustrates the smart meter structure, connecting a micro controller with two communication modules (HAN and DNT 900MHz radio) and the meter board for reading and storing usage data. Figure 8 is a photograph of the smart meter, and Figure 9 is a photograph of the communication board.

6.7.1 Smart Meter Network Configuration

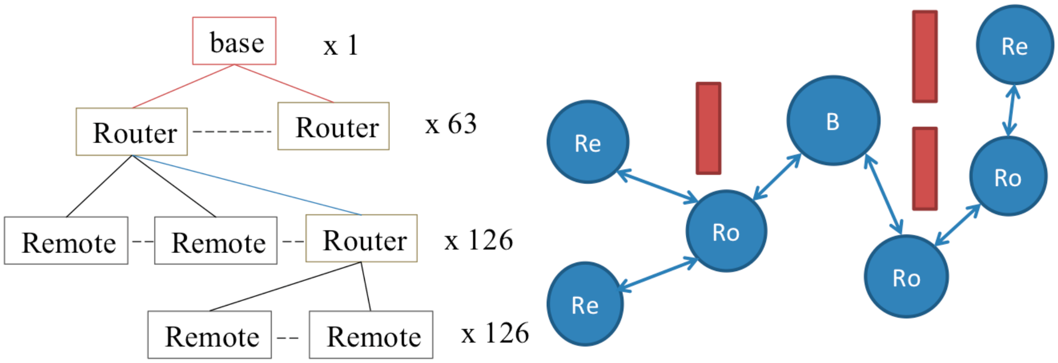
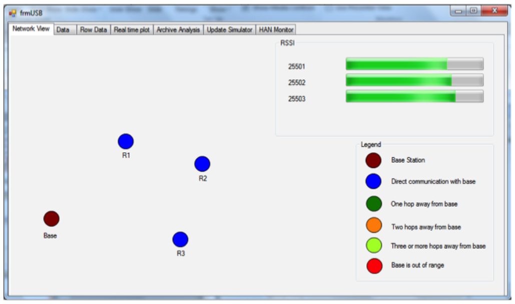
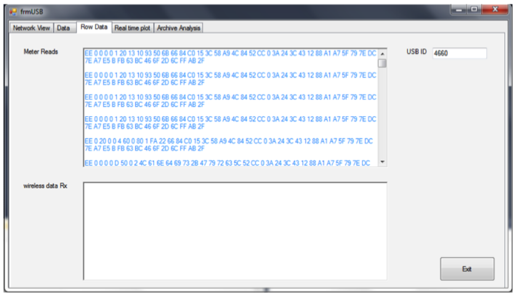


Figure 10: Smart Meter Network Configuration

Figure 10 illustrates the tree-based routing arrangement used in the CKMS smart meter network. Depending on the configuration, each node may act as a router, remote node, or both.

6.7.2 Smart Meter Network Monitoring





Meter Reads

```
EE 0 0 0 0 1 20 13 10 93 50 6B 66 84 C0 15 3C 58 A9 4C 84 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
7E A7 E5 B FB 63 BC 46 6F 2D 6C FF AB 2F

EE 0 0 0 0 1 20 13 10 93 50 6B 66 84 C0 15 3C 58 A9 4C 84 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
7E A7 E5 B FB 63 BC 46 6F 2D 6C FF AB 2F

EE 0 0 0 0 1 20 13 10 93 50 6B 66 84 C0 15 3C 58 A9 4C 84 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
7E A7 E5 B FB 63 BC 46 6F 2D 6C FF AB 2F

EE 0 0 0 0 1 20 13 10 93 50 6B 66 84 C0 15 3C 58 A9 4C 84 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
7E A7 E5 B FB 63 BC 46 6F 2D 6C FF AB 2F

EE 0 20 0 0 4 60 0 80 1 FA 22 66 84 C0 15 3C 58 A9 4C 84 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
7E A7 E5 B FB 63 BC 46 6F 2D 6C FF AB 2F

EE 0 0 0 0 D 50 0 2 4C 61 6E 64 69 73 2B 47 79 72 63 5C 52 CC 0 3A 24 3C 43 12 88 A1 A7 5F 79 7E DC
```

USB ID 4660

wireless data Rx

Figure 11: Net+MeterMon Network Summary

Figure 12: Net+MeterMon Data Capture

The Net+MeterMon tool provides a high level overview of the smart meter network. It allows users to monitor and view data at various points within the network, view network statistics and capture simulation data.

6.8 Sypris Electronics Cyber Range Modeling Testbed

The Cyber Range Modeling and Simulation Environment from Sypris Electronics is a dynamic virtualization platform for interacting with virtual networks composed of both software and hardware components. The primary function of the Cyber Range as a testbed is for evaluating the CKMS in terms of performance and scalability.

6.8.1 Cyber Range Architecture

The Cyber Range Architecture is powered by a virtualization platform that provides a common framework for integration of components needed to support the core modules. As shown in Figure 13, the architecture provides a interface layer for integration with external hardware and software components. The primary interaction the user is provided by a web-based interface for administration, management and monitoring, and general user access. The virtualization environment allows the security of simulated network configurations to be assessed in a safe and sandboxed manner, allowing new systems to be evaluated before deployment.

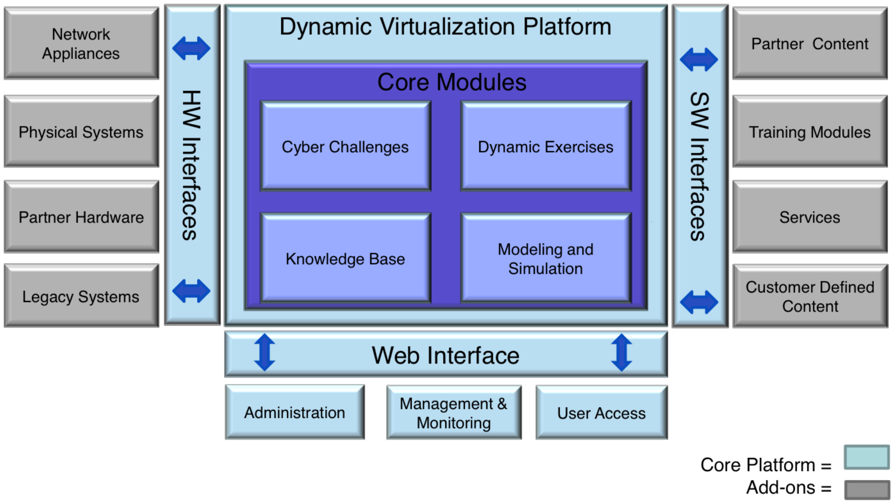


Figure 13: Cyber Range Architecture

6.8.2 Cyber Range Core Modules

The Cyber Range includes four core modules for training and modeling and simulation features. A summary of these modules are as follows:

- **Knowledge Base:** The knowledge base is a collection of cyber security information designed to help train cyber security professionals. The knowledge base provides background information on core concepts, and provides walk-throughs for many cyber attack vectors.

- **Cyber Challenges:** The cyber challenge module allows cyber security professionals to work through solo exercises designed to exploit vulnerabilities in virtual network environments.

- **Dynamic Exercises:** The dynamic exercises module allows cyber security professionals to work in groups in an interactive manner. For example, one team may act as attackers, while the other attempts to defend a virtual network.

- **Modeling & Simulation:** The Cyber Range allows users to design, deploy, and interact with custom network configurations in a virtualized setting.

6.9 Key Technical Features

The key features of the CKMS solution include:

- An XML template engine for processing device key requests based on device type.

- A generic key management solution not tied to any specific vendor, providing applicability to generalized future extensions.

- FIPS 140-2 Level 3 validated HSM for the generation and protection of certificates and key material at the server.

- Generalized framework for handling multiple device types and communication protocols provides versatility.

- Multiple messaging scenarios for integration with the Utility provides versatility.

- Modular architecture design for security module integration facilitates generalized future extensions.

- API for multiple UI type designs and integration based on the requirements of the Utility.

- AMI Testbed with In-Loop Landis+Gyr Hardware Meter Boards provides a realistic testing and simulation environment.

- Support for customized testing scenarios, such as new hardware components or security technologies (e.g., algorithms, key management schemes, etc.).

- Network meter nodes provides communication paths to each other as well as Home Area Networks (HANs).

7 Demonstrations

Below is a summary of the CKMS external demonstrations performed during the project. These demonstrations include public conferences and DOE customer demonstrations.

- DistribuTECH Conference
  - San Diego Convention Center, CA
  - January 29-31, 2013
  - Demonstrated initial CKMS integrated with the vCore architecture to the electric utility audience as part of the DOE CSEDS booth.
- RSA Conference
  - Moscone Center, San Francisco, CA
  - February 24-28, 2013
  - Demonstrated initial CKMS integration with the vCore architecture to the general security community as part of the Sypris Electronics booth.
- Mid-Year Demonstration
  - Sypris Research Center, West Lafayette, IN
  - June 11, 2013
  - Demonstrated integration with the Purdue SMIL Testbed
- End-of-the-Year Demonstration
  - Sypris Research Center, West Lafayette, IN
  - December 2013
  - Demonstrated integration with Sypris Electronics Cyber Range for scalability and testing of the CKMS server

7.1 2013 Mid-Year Demonstration

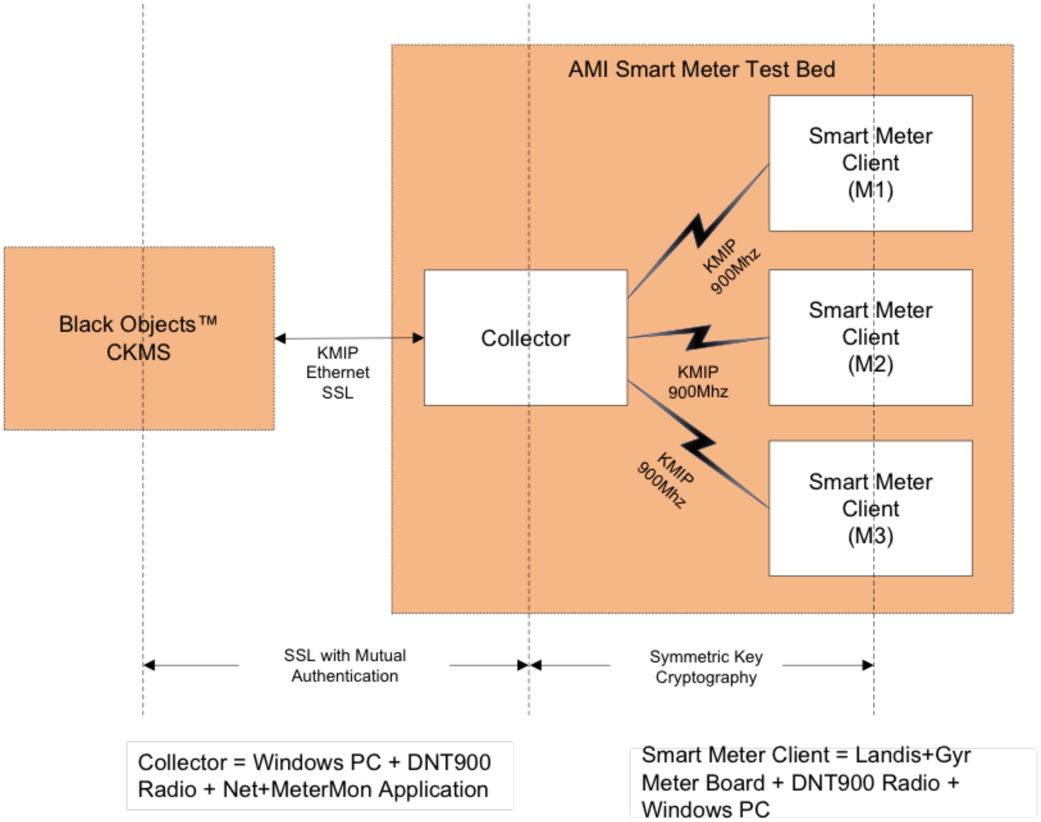
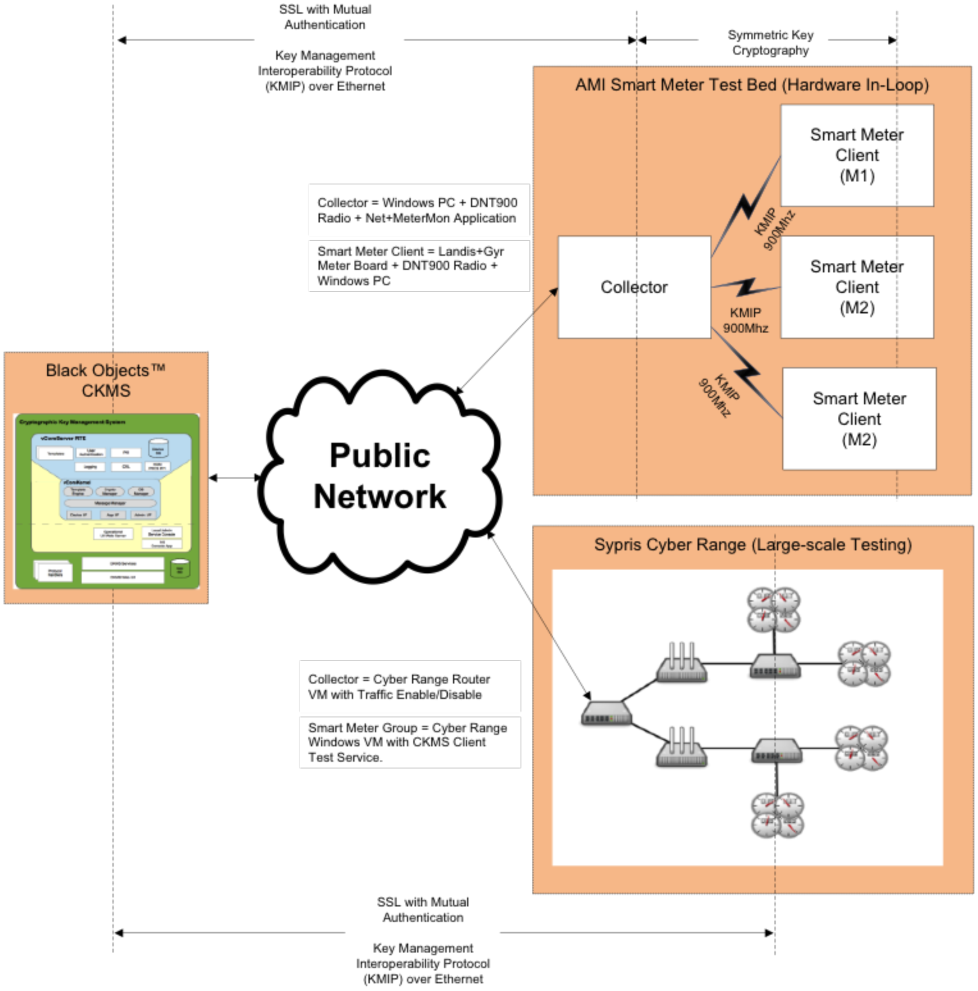

AMI Smart Meter Test Bed
Smart Meter Client (M1)
Smart Meter Client (M2)
Smart Meter Client (M3)
Black Objects™ CKMS
Collector
KMIP Ethernet SSL
KMIP 900Mhz
KMIP 900Mhz
KMIP 900Mhz
SSL with Mutual Authentication
Symmetric Key Cryptography
Collector = Windows PC + DNT900 Radio + Net+MeterMon Application
Smart Meter Client = Landis+Gyr Meter Board + DNT900 Radio + Windows PC

Figure 14: Mid-Year Demonstration Overview

The 2013 Mid-Year Demonstration included the following features of the CKMS:

- Symmetric and Asymmetric Key Management Functions
- Integration of vCoreServer
- Integration with AMI Smart Meter Testbed
- Integration of Hardware Security Module
- Key Management Interoperability Protocol (KMIP)
- Web-based User Interface for Device Management

7.2 Final Demonstration


SSL with Mutual Authentication
Key Management Interoperability Protocol (KMIP) over Ethernet
Symmetric Key Cryptography
AMI Smart Meter Test Bed (Hardware In-Loop)
Smart Meter Client (M1)
Smart Meter Client (M2)
Smart Meter Client (M2)
Collector
KMIP 900Mhz
KMIP 900Mhz
KMIP 900Mhz
Black Objects™ CKMS
Public Network
Sypris Cyber Range (Large-scale Testing)
SSL with Mutual Authentication
Key Management Interoperability Protocol (KMIP) over Ethernet

Collector = Windows PC + DNT900 Radio + Net+MeterMon Application

Smart Meter Client = Landis+Gyr Meter Board + DNT900 Radio + Windows PC

Collector = Cyber Range Router VM with Traffic Enable/Disable

Smart Meter Group = Cyber Range Windows VM with CKMS Client Test Service.

Figure 15: Final Demonstration Overview

The final demonstration included the following features of the CKMS:

- CKMS integrated with Cyber Range to support large scale testing of the CKMS protocol and performance.
- The AMI network was modeled using Cyber Range Modeling & Simulation Canvas.

- The AMI network was deployed to the virtual environment with an external interface to the CKMS server.
- Current AMI components include Collectors and Smart Meters:
  - Collectors are similar to network routers, and collect data from a set of smart meters.
  - Smart Meters are managed as Groups for simplifying the creation of large scale networks in the Cyber Range.
- Provides a framework for testing CKMS with various key management technologies and network architectures.

7.3 Performance Results

The Cyber Range was successfully used for testing the CKMS capacity for simultaneous device connections. Before integration with the Cyber Range, tests were limited to approximately 1,000 simultaneous device connections. After integration with the Cyber Range, the capacity of the CKMS was at least *doubled* using updated software optimized through collaboration with Valicore.

The limitation refers to the number of simultaneous key management operations occurring at any given time. The total number of end devices capable of being supported by a single CKMS server depends on the frequency of the key update operations (i.e., the cryptography period policy). More frequent key update operations reduce the number of devices a single CKMS server can support, while less frequent key updates extend the server's capacity.

8 Summary of Project Objectives

- **Leverage Existing Infrastructure for Cryptographic Key Distribution**
  - Key Management Interoperability Protocol (KMIP) is a low overhead open protocol developed for interoperability between the enterprise key management system and the end devices.
  - KMIP separates key generation and distribution functions, allowing optimal usage of the existing network infrastructure.
  - Device API and Template engine provide flexibility in supporting device types, network infrastructure capabilities, and device keying formats.
  - The HSM supporting key synchronization enables flexible deployments with distributed servers.
  - The HSM supports ”Functionality Modules” that can be loaded to support legacy algorithms.
  - Initial version of the CKMS is compatible with Ethernet-based interfaces, but can be expanded to handle other interfaces.
- **Deployment of Multiple Open Standard Algorithms to Adapt to Risk Exposure**
  - Integrated FIPS validated HSM with Standard PKCS#11 Interface
    - Supports upgrade of new algorithms via ”Functionality Modules”
    - Supports standard PKCS#11 interface for multiple HSM configurations
  - Template engine supports upgrading to new device cryptographic key formats without modifying the CKMS vCore Kernel
  - Open standard protocol (KMIP) for all key management operations between CKMS and the end device
  - Base algorithms are those supported by the SafeNet Luna PCI-E HSM

- **Scalable to Support Operator Workload Distribution and Large Networks**
  - vCore Application API may be used for distributed workload or multiple user interfaces
  - HSM supports synchronization capabilities for distributed key generation
  - Minimal user intervention required for KMIP operations
  - Existing user interface supports bulk device import and key/certificate export features
  - Cyber Range used for performance testing of the CKMS for large numbers of end nodes
- **Add Minimal Traffic Bandwidth to Existing Interface**
  - HSM supports synchronization capabilities for distributed key generation
  - KMIP separates key generation and key distribution operations for balancing server and network bandwidth
  - Symmetric algorithms with key updates based on the device policy
  - Web user interface is separate and does not impact the traffic on the device interface
  - Symmetric key management approach is more efficient for smart grid deployments than a PKI approach, eliminating the need to negotiate a new key for each new session
- **Minimize Interaction between CKMS and Device for Key Distribution**
  - Supports management of symmetric keys that are updated based on the device policy
  - KMIP key updates are performed with two messages (Generate Key, Request Key) that may be done asynchronously based on network availability
  - New key management schemes (such as CL-PKC) may offer significant reduction in interaction between the key management system and the end device

- **Minimize Time to Recover from a Key Compromise Situation via Distribution**
  - KMIP protocol separates key generation and key distribution operations to:
    - Minimize binding of server capacity to the network for key generation operations
    - Support simultaneous key distribution to end devices
  - HSM supports multiple servers generating keys at different locations with the synchronization feature
  - New key management schemes (such as CL-PKC) may offer significant reduction in interaction between the key management system and the end device for compromise recovery
- **Eliminate Need for Continually Growing Certificate Revocation List (CRL)**
  - The CKMS supports the management of symmetric-based keys, where keys are updated based on the policy of the device
  - CL-PKC key management scheme eliminates device certificate management overhead at the utility
- **Support Symmetric Cryptographic Algorithms for Maximized Data Throughput**
  - CKMS supports symmetric key management, which is more efficient for smart grid deployments than a PKI approach, eliminating the need to negotiate a new key for each session
  - Architecture supports updates to the cryptographic algorithms and key formats
    - Algorithms loaded into the HSM via ”Functionality Modules”
    - Key formats are loaded through the vCore Template Engine
  - Demonstrated capabilities included symmetric key management operations with resource constrained devices
- **Remove the Processing Burden and Security Weakness from End Devices**

- CKMS supports centralized key generation
  - Security enforced by the HSM
  - Flexible key formats supported by the vCore Template Engine
- KMIP separates Key Generation and Key Distribution functions allowing support for key generation and escrow building

- **Support Flexible and Dynamic Smart Grid Network Communications Architecture**
  - CKMS Device API supports multiple device types and network communications interface
  - Dynamic generation and distribution of keys depending on the device needs
  - Facilitates translating shared data between two devices with different protocols and keys
  - Initial version of CKMS is compatible with Ethernet-based interfaces, but can be expanded to handle other interfaces
- **Support Cryptographic Module Updates of Smart Grid Devices**
  - Device API and Template engine support for cryptographic requirements of each device type
  - HSM with support for ”Functionality Modules” that can be developed and loaded to support new algorithms
  - Base algorithms are those supported by the SafeNet Luna PCI-E HSM
- **Provide Utility Operations with Control of Root of Trust for Key Management System**
  - Integrated FIPS 140-2 Level 3 HSM provides the highest level of security and root of trust for the following CKMS features
    - Protection of the CKMS Root Key
    - Device Certificate Generation
    - Device Certificate Signatures

        - Symmetric Key Generation
        - Random Number Generation for Cryptographic Operations
    - Enforces low level security for deployments with distributed server configurations through HSM data synchronization

- **Prove System in Smart Grid Network Environments**
    - Demonstrated CKMS integrated with the Purdue SMIL Testbed (June 2013)
    - Demonstrated CKMS integrated with the Cyber Range for large scale network testing (December 2013)
    - Recommended Future Work:
        - Integrate the CKMS with a selected vendors metering system in a sandboxed environment (e.g., Landis+Gyr Command Center)
        - Challenge here is to identify a vendor interested in performing the integration as they tend to offer a key management solution with their product line

- **Maintain Confidentiality and Integrity during Loss of Network Connectivity**
    - KMIP separates Key Generation and Key Distribution functions allowing optimal usage of the existing network infrastructure
    - HSM supports synchronization of data between multiple servers for distributed generation and distribution of keys
    - All key generation performed in HSM-protected environment
    - HSM supports the confidentiality of symmetric keys via encryption of the key for transfer over the network
    - Template Engine supports the building of the key format which may include a checksum or CRC for key integrity

9 Inventions, Publications, and Conference Reports

9.1 2013 Publications

- Cryptographic Key Management for Smart Power Grids
  - M. Nabeel, J. Zage, S. Kerr, E. Bertino, A. Kulatunga, S. Navaratne, M. Duren
- Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures
  - S.-H. Seo, X. Ding, E. Bertino; IEEE SmartGridComm 2013 Symposium
- An Efficient Certificateless Cryptography Scheme without Pairing
  - S.-H. Seo, M. Nabeel, X. Ding, E. Bertino; ACM CODASPY 2013 Conference
- Information Security Analysis for CKMS Using Game Theory and Simulation
  - R. K. Abercrombie, F. T. Sheldon, B. G. Schlicher; 1st International Symposium on Resilient Cyber Systems, 2013
- Failure Impact Analysis Using Cybernomic Analytics
  - R. K. Abercrombie, F. T. Sheldon; Milibo Webinar
- Authentication and Key Management for Advanced Metering Infrastructures Utilizing Physically Unclonable Functions
  - M. Nabeel, S. Kerr, X. Ding, E. Bertino; IEEE SmartGridComm 2013 Symposium

9.2 2014 Publications

- A Pairing-free Certificateless Hybrid Sign-Cryption Scheme for Advanced Metering Infrastructures
  - S.-H. Seo, J. Won, E. Bertino; Poster, ACM CODASPY 2014 Conference

- Effective Key Management in Dynamic Wireless Sensor Networks for Monitoring Applications
  - Submitted for Publication
- Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation
  - R. K. Abercrombie, B. G. Schlicher, F. T. Sheldon; HICCS-47, 2014 Conference

10 Commercialization Possibilities

10.1 Integration with Commercial Smart Meter Network

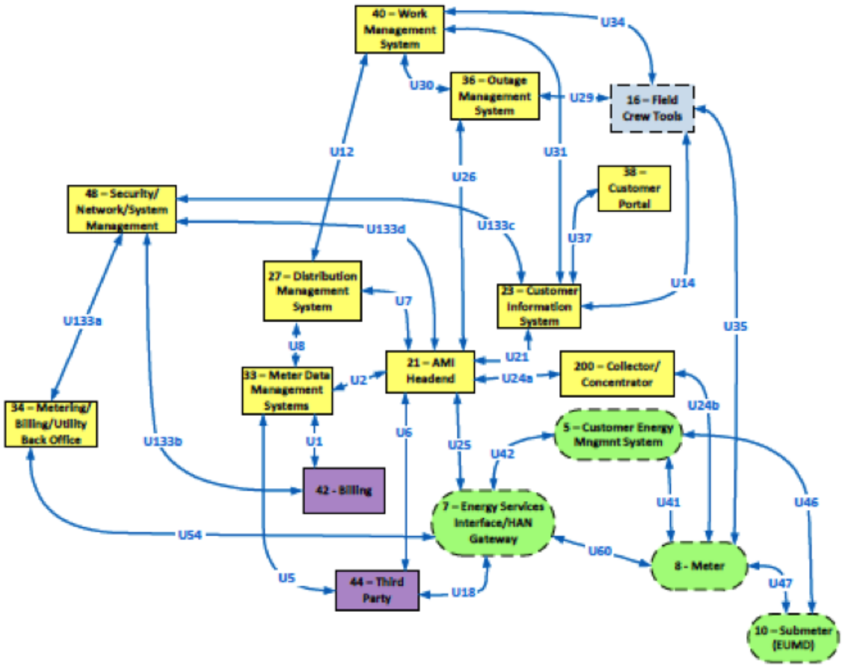

40 – Work Management System
36 – Outage Management System
16 – Field Crew Tools
38 – Customer Portal
48 – Security/ Network/System Management
27 – Distribution Management System
23 – Customer Information System
21 – AMI Headend
200 – Collector/ Concentrator
33 – Meter Data Management Systems
34 – Metering/ Billing/Utility Back Office
5 – Customer Energy Mngmnt System
42 - Billing
7 – Energy Services Interface/HAN Gateway
8 - Meter
44 – Third Party
10 – Submeter (EUMD)
U34
U30
U29
U12
U26
U31
U37
U133d
U133c
U14
U7
U133a
U8
U21
U2
U24a
U35
U24b
U6
U1
U133b
U25
U42
U41
U46
U54
U60
U5
U18
U47

Figure 16: AMI Component Spaghetti Diagram

A potential avenue for commercialization of the CKMS project is integration with the commercial smart meter network. The existing smart meter network infrastructure is complex, and its details vary depending on utility and equipment vendors. Through collaboration with EPRI, the spaghetti diagram illustrated in Figure 16 was distilled to those components most closely associated with the AMI.

As part of future work, the CKMS could be integrated with an existing vendor's metering system in a sandboxed environment. For example, integrating CKMS with the Landis+Gyr command center would demonstrate feasibility on an existing system.

10.2 Key Management Product Commercialization

The CKMS has been designed as a generic key management solution, and is not tailored to any particular vendor requirements or network structure (e.g., Template Engine, KMIP for Key Distribution, PKCS#11 Interface for HSM). Thus, the CKMS is applicable to many other applications and use cases, such as:

- Handling sensitive (but not classified) information for the Missile Defense Agency
- Automotive security applications
- Securing transactions in a financial banking application
- Civil Airspace Unmanned Aerial Vehicles (UAVs)

These potential synergies provide a strong benefit to the DOE as the CKMS product continues to mature into a product for commercialization. A critical step towards this goal is the integration of the CKMS with one or more smart meter vendor systems.

11 Future Work

11.1 Enhanced Modeling and Simulation Smart Meter Group

The current smart meter group implementation is focused on simulating the security interface and the KMIP protocol between the CKMS server and smart meter devices. In the future, the smart meter group could also include network and device performance for common AMI network topologies, such as a mesh network.

The benefits would include a quantitative assessment of the CKMS and key management performance in relation to network delays, smart meter processing time, the number of hops between the CKMS server and end nodes, and encryption or authentication approaches.

11.2 Integration with Purdue SMIL Training and Research Platform

The Purdue University SMIL is currently developing an operational training and applied research platform for distributed resource integration into the smart grid in conjunction with Landis+Gyr. The platform supports the development of technologies and operational methodologies for power management, big data management, and key management.

Integrating the CKMS and Cyber Range into this platform would provide many benefits, such as:

- A new key management scheme and its impact on smart grid components
- The impact of cyber-attacks on utility and smart grid components
- The development of counter measures to defend against cyber attacks targeting utility and smart grid components
- Advanced training for smart grid technologies within a hybrid environment, including both in-loop hardware and a virtual smart grid network

11.3 Implementation of CL-PKC Key Management Schemes

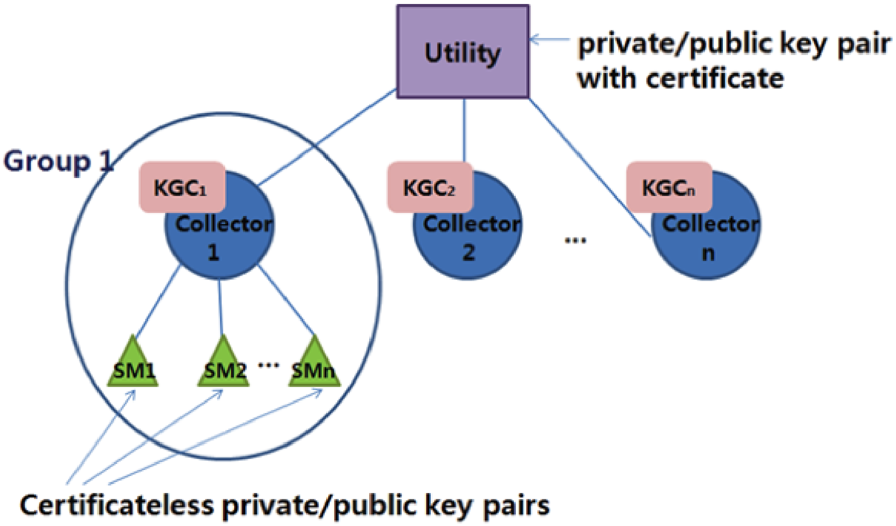


Figure 17: Certificateless Public Key Cryptography

Another potential future research direction is investigating the application of *certificate-less* public key cryptography to the smart meter network. In this scenario, the Utility holds its own public/private key pairs with certificates. The smart meters hold certificate-less key pairs. Thus, the key management burden is transferred from the Utility to the Collectors, which enhances options for scalability. This configuration is illustrated in Figure 17. The benefits of this direction include scalability testing of the certificate-less public key approach against the current CKMS and AMI network construction.