Smart Grid Cryptographic Key Management

Scalable cryptographic key management to secure data and communications for millions of smart devices in the energy sector

Background

As smart technologies such as those used by the advanced metering infrastructure (AMI) are increasingly deployed, securing data at rest and in transit is crucial.

Cryptography ensures the confidentiality, integrity and authenticity of data used in most modern cyber physical systems, such as critical control data and personally identifiable information. The protection of cryptographic keys used to encrypt and decrypt the data is vital to the integrity of any encryption system. If a key is compromised, then the information and systems it was intended to protect are no longer secure.

Energy delivery systems are large, geographically dispersed, complex systems of heterogeneous devices and communications media. Systems such as the AMI require a key management approach that must handle very large numbers of keys and operate in a very diverse environment.

Barriers

- Energy delivery system architectures are complex and widely distributed
- Smart meters are increasing the complexity and interconnectivity of the energy delivery system, and next-generation cybersecurity solutions are needed to further strengthen existing protections against the resulting increased exposure to potential threats
- The cryptographic key-count to device ratio is increasing as meters begin interfacing with other systems such as Home Area Networks (HANs), Electric Vehicles (EVs), and Distributed Generation systems

Project Description

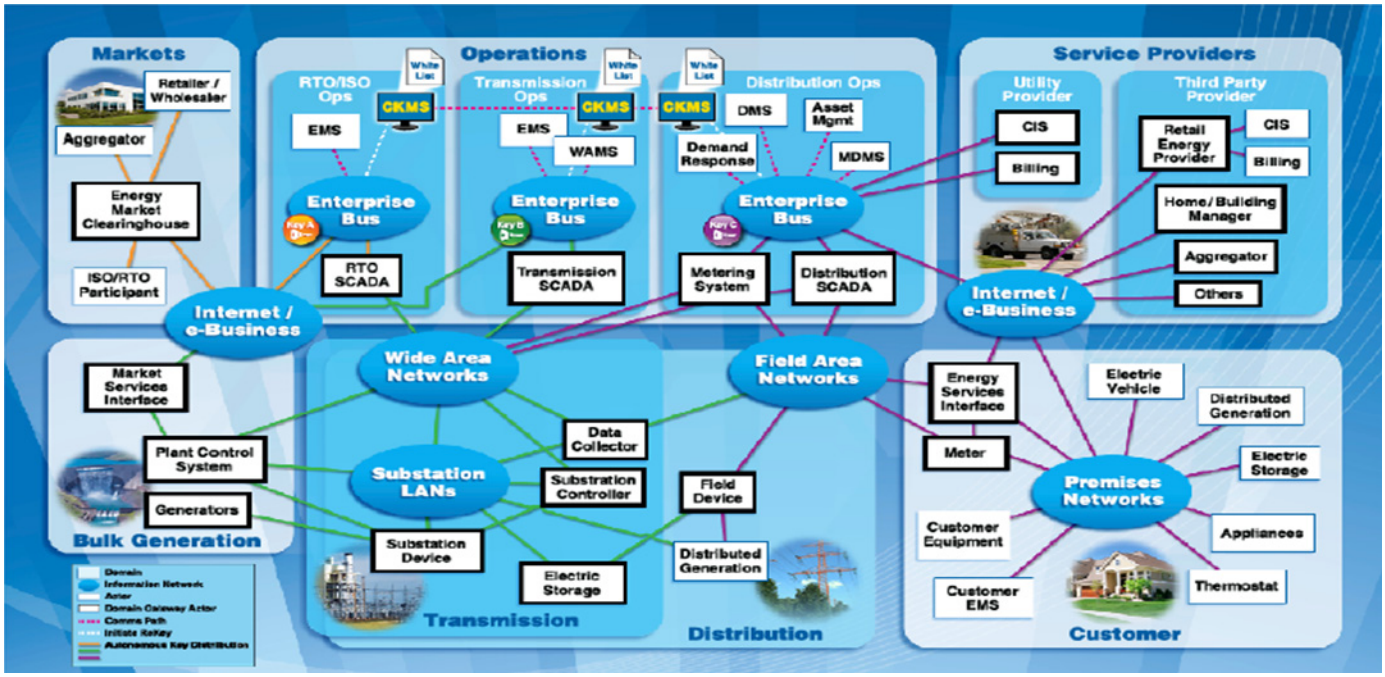
This project will produce the Cryptographic Key Management System (CKMS) for the secure management of cryptographic keys for energy sector infrastructure. The CKMS leverages the best practices of existing Department of Defense (DoD) key management systems deployed today to protect high-value information. The system will help energy control systems recover quickly from a cryptographic key compromise and fend off cyber attack by using an autonomous key distribution scheme. The CKMS will be cost-effective, easy to use, and highly capable.

Benefits

- Builds on established and successful DoD key management systems
- Provides tools for the energy sector to confront the numerous challenges of safeguarding critical energy control systems
- Facilitates realization of the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* for improving cybersecurity in the energy sector

Partners

- Sypris Electronics, LLC
- Purdue University Center for Education and Research in Information Assurance and Security
- Oak Ridge National Laboratory
- The Electric Power Research Institute
- Valicore Technologies



Technical Objectives

This project involves research, development and demonstration geared toward producing a robust, user-friendly and cost-effective cryptographic key management system.

- Develop the CKMS and Trusted Certificate Provisioning System
- Demonstrate the initial technologies for the secure management of cryptographic keys within a simulation environment that represents energy sector infrastructure
- Develop new, low-cost anti-tamper technologies to protect cryptographic keys and secure encryption functions
- Conduct analysis of the results that will lead to an understanding of the scalability, performance and cost versus benefit of the system
- Test the technologies in a laboratory environment using representative Smart Grid devices to measure the improvements in scalability, performance and cost versus benefit
- Perform a final analysis to verify acceptable scalability, performance and cost versus benefit

End Results

Project results will include:

- A dynamic cryptographic key management solution that increases the ability of energy control systems to withstand cyber attacks
- Technology that is scaled to secure communications for the millions of smart meters within the advanced metering infrastructure
- Advancements in low-cost, high assurance cryptographic hardware designs

Content last updated: August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Ron Frank
Program Manager
Sypris Electronics, LLC
813-972-6101
ron.frank@sypris.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov