Department Of Energy
Cryptographic Key Management System

Integrated Customer Solutions. From Thought to Finish

Partnering to Deliver Best Practices and Technologies to Meet the Emerging Needs of our Country and Customers
Project Description

Produce the Cryptographic Key Management System (CKMS) for the secure management of keys for the energy sector infrastructure

- Leverage DoD best practices in key management to the energy sector
- Protect high value data, command and control information, and fend off cyber attacks
- Secure generation, distribution, and revocation of keys to smart grid domains
- Current focus on Advanced Metering Infrastructure (AMI)
Department of Energy (DOE) Cybersecurity for Energy Delivery Systems (CEDS)

- CEDS projects are funded through the DOE Office of Electricity Delivery and Energy Reliability R&D Program
- 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
Project Team

- Sypris Electronics – Prime contractor to DOE
- Purdue University Center for Education and Research in Information Assurance and Security (CERIAS)
- Purdue University Smart Meter Integration Lab (SMIL)
- Oak Ridge National Laboratory (ORNL)
- Electric Power Research Institute (EPRI)
- Valicore Technologies
Recent Demonstration

- Symmetric and Asymmetric Key Management Functions
- Integration of vCoreServer
- Integration with AMI Smart Meter Testbed
- Integration of Hardware Security Module (HSM)
- Key Management Interoperability Protocol (KMIP)
- Sample web-based user interface for device management

Collector = Windows PC + DNT900 Radio + Net+MeterMon Application
Smart Meter Client = Landis+Gyr Meter Board + DNT900 Radio + Windows PC