

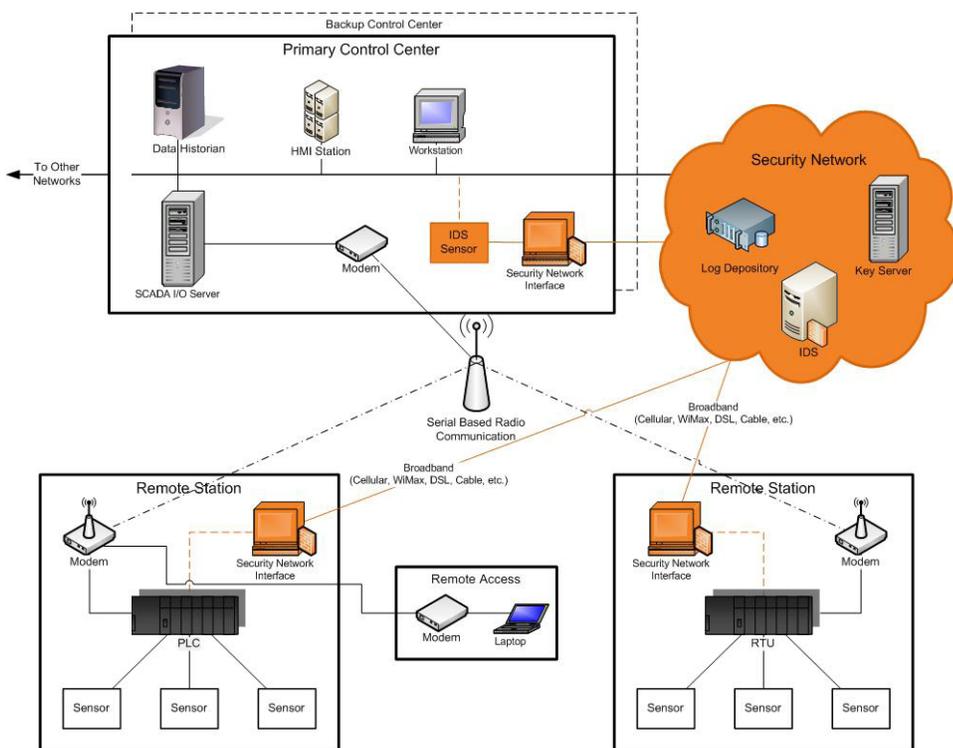


# Cryptographic Trust Management

The Cryptographic Trust Management System project's purpose is to design a system to facilitate the integration of cryptographic technical security controls into control system networks while still maintaining an affordable operational cost. Secure communication devices, protocols, and applications require the ability to manage cryptographic key material. Without well managed key material, secure communication methods are at best deployed in a limited fashion, and at worst, they are deployed insecurely. A cryptographic trust management system must be designed that supports the operational requirements and personnel capabilities of asset owners. The system must also continue to function in the event of a loss

The introduction of cryptography into control systems represents a significant challenge to vendors, asset owners, and standards bodies. Due to physically separated infrastructure, these environments historically have not had to contend with cyber security concerns. Managing and operating cyber security solutions can be difficult and overwhelming.

The lack of a scalable technology to manage cryptographic keys and trust for control systems hinders the deployment of vendor products that secure control system communications.



of communication or equipment failure; the technology cannot prevent operational control of the infrastructure.

For a cryptographic trust management system to function, standards for device identity, device/entity authentication and authorization, key management processes, and third party connectivity trust negotiation must be established. This project attempts to define suitable current standards and create protocols when necessary to fulfill these needs.

## PROBLEM DOMAIN

- » Too many application silos with their own management processes
- » Scalability, both in operation and management, of IT key management solutions
- » Subsections of environment must continue to operate during times of lost communication
- » Cryptographic processes must minimize impact on reliability
- » Lack of cryptographic trust management solution hinders the adoption and integration of security applications

## SOLUTION

- » Centralize cryptographic material generation to accommodate embedded device hardware limitations and guarantee policy-enforced levels of security
- » A centralized secure storage and backup process of cryptographic material

Application	Key Type	Relative Scale
Automated Meter Reading	Shared and/or Public/Private	Millions
Secure E-mail	Public/Private	Hundreds
Authenticity of log files	Public/Private	Dozens
Critical information protection (asset lists, cyber asset lists, etc.)	Public/Private	Dozens
SSL connection for web-based applications	Public/Private	Dozens
Secure protocols (ICCP, DNP)	Shared and/or Public/Private	Thousands
Legacy encryption or authentication solutions	Shared and/or Public/Private	Thousands
Embedded encryption or authentication solutions	Shared and/or Public/Private	Thousands
Engineering access to field devices	Shared and/or Public/Private	Thousands
SCADA radio networks	Shared	Hundreds+
Other wireless technologies	Shared and/or Public/Private	Hundreds+
Remote access (staff, vendor or site) via VPN, SSH, or TS	Public/Private	Hundreds

### Possible Industry Security Applications

- » Automate device-to-device key management services to reduce management burden
- » Centralize AAA services while providing temporary distributed AAA capability
- » Increase assurance of third-party connectivity through per connection trust negotiation

## PNNL APPROACH

- » Leverage Lessons Learned in cell and payment card industries
- » Use work from similar efforts, such as OASIS KMIP and interface with NIST
- » Leverage PNNL expertise with PKI and SSCP deployments

## WHY THIS SOLUTION IS BETTER

- » Designed around the control system environment and its constraints
- » Focuses on relieving some of the security application management burden from the utility
- » Built upon open standard protocols (where feasible)

**For more information, contact:**

**Thomas Edgar**  
 Pacific Northwest National Laboratory  
 Thomas.Edgar@pnl.gov



Proudly Operated by **Battelle** Since 1965