U.S. DEPARTMENT OF ENERGY

PNNL-18744

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Cryptographic Trust Management Requirements Specification

Version 1.1

TW Edgar

September 2009

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the Office of Scientific and Technical Information,

P.O. Box 62, Oak Ridge, TN 37831-0062;ph: (865) 576-8401fax: (865) 576-5728email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 ph: (800) 553-6847 fax: (703) 605-6900

email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

PNNL-18744

Cryptographic Trust Management Requirements Specification

Version 1.1

TW Edgar

September 2009

Prepared for
the U.S. Department of Energy, OE-10
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Revision History

Release	Date	Comments
0.1	07/11/2009	Initial draft
0.2	07/17/2009	Second draft
0.5	08/03/2009	Team review draft
0.7	08/14/2009	Second Team review draft
0.9	08/31/2009	Technical Edit ready draft
1.0	09/08/2009	
1.1	09/28/2009	Addressed comments of industry technical reviewers

Contents

Introduction

The Cryptographic Trust Management (CTM) Project is being developed for Department of Energy, OE-10 by the Pacific Northwest National Laboratory (PNNL). It is a component project of the NSTB Control Systems Security R&D Program.

Specification Purpose and Scope

This Requirements Specification (RS) specifies the essential capabilities required of the CTM Project through pilot rollout. The purpose of this document is to clarify for the Department of Energy and the CTM development team the results that must be achieved by the CTM product suite. Any illustrative model presented in this document is used solely to explain CTM requirements and is NOT intended to address design or implementation issues.

This RS is an unordered, un-prioritized list of requirements. The requirements in this document will direct the design and implementation of the proof of concept system. However, it is understood that it may not be possible, due to resource and technical constraints, to fully comply with all of the requirements defined. When a design or implementation choice is made that will not meet a requirement the justification and impact will be documented.

Cryptographic Trust Management Purpose and Scope

The purpose of this project is to create a software application to manage cryptographic keys to support the deployment of technologies developed to meet multiple Roadmap goals.

The lack of a scalable technology to manage cryptographic keys for control systems hinders the deployment of vendor products to secure control system communication. The prime example of this critical missing element is the failed deployment of products designed to the American Gas Association (AGA) 12 Cryptographic Standard. Without an industry acceptable, scalable, secure, and robust mechanism to create cryptographic keys that supports the operational requirements of critical infrastructure asset owners, no cryptographic solution will be widely deployed. Comments received during the 2008 PCSF conference and the peer reviews for the Hallmark project echo this sentiment. Industry requires a cryptographic key management solution to further the deployment of technical solutions and to eliminate the risk associated with control system communication.

The introduction of cryptography into control systems represents a significant challenge to vendors, asset owners, and standards bodies. The cryptographic goals for control systems differ significantly from corporate IT or Internet sites. The security objectives of IT Systems in order of importance are confidentiality, integrity, and lastly availability. In contrast, the security objectives for control systems are:

- Availability
- Integrity
- Confidentiality

In addition, the use of cryptography in control systems must support the multiple operational needs of asset owners without adversely affecting reliable operations or personnel safety. The cryptographic key

management problem is made more complicated by the number of vendors creating security products, regulatory requirements to identify and protect critical information, and the automation of previously manual processes (e.g., automated meter reading).

Another hurdle to overcome is the potential size of a control system network. Managing cryptographic keys for a small utility with 30 substations can be done without automation. Managing keys for an automated meter reading environment with millions of smart meters cannot.

The following is a sample of the potential application of cryptographic solutions a single utility must manage:

- Automated Meter Reading
- Validation of log files
- SSL connection for web based applications
- Secure ICCP or DNP
- Bump in the wire serial encryption or authentication devices
- Embedded or integrated authentication solutions
- Secure engineering access to field devices
- SCADA Radio networks
- Other wireless technologies (802.11, Bluetooth)
- Remote access (staff, vendor, or site) via VPN or SSH

The creation of a control system key management application will provide a key building block to allow the following Roadmap goals to be met:

1. Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy.
2. Next-generation control system components and architectures that offer built-in, end-to-end security will replace older legacy systems.
3. Secure connectivity between business systems and control systems within a corporate network.

The scope of this project will focus on the control system network. The focus will be to support systems and services only within the boundaries of the control system network and will not focus external enterprise applications.

Reference and Resources

All documents referenced in this requirements specification are listed in Appendix D: References and Resources.

Document Overview

Product Overview – This section provides a descriptive overview of the CTM product suite, its users and operating environment, and general factors that affect requirements. It lays the foundation for understanding the specific requirements that follow.

Specific requirements are specified in the following categories:

1. Functional Requirements
2. External Interface Requirements

3. Design Constraints
4. Performance Requirements
5. Usability Requirements
6. Reliability Requirements
7. Security Requirements
8. Availability Requirements
9. Portability Requirements
10. Supportability Requirements
11. Other Requirements

Appendices

Appendix A: Use Cases gives example scenarios of how the CTM product suite is expected to be used.

Appendix B: Definitions, Acronyms, and Abbreviations lists a glossary of terms that appear in the RS.

Appendix C: NSTB Advisory Board and Technical Team Members identifies the members of the National SCADA Test Bed Advisory Board and PNNL technical team.

Appendix D: References and Resources identifies documents and other information sources relevant to the CTM project and RS.

Product Overview

The following overview of the CTM product suite provides context for the specific requirements presented in later sections. The purpose of this information is to make the specific requirements easier to understand. All specific requirements are numbered in later sections.

NSTB Goal: No explicit goal in the Roadmap document mentions the CTM project. However, this project directly supports Roadmap goals and milestones to deploy next-generation control systems with cost-effective methods to secure communication between control centers and remote devices by FY 2013.

Roadmap Challenges: Without adequate trust management, secure communication methods will not be widely deployed by control system operators.

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, insecurely. This project will identify requirements for cryptographic key management for the entire control system, design and develop a control system-specific solution for cryptographic trust management, and create a best practices guide for asset owners to implement the technology. The end result will be a CTM system that supports both intra- and inter-control system communication for heterogeneous applications, protocols, and devices.

Using its Electric Infrastructure Operations Center (EIOC) and the future Secure Energy Laboratory, PNNL will design, develop, and demonstrate a CTM system. To facilitate vendor adoption of the CTM system and vendor interoperability, the PNNL CTM solution will utilize a standard interface for vendor products.

The PNNL project team will utilize industry advisors to guide research and development activities.

Product Functions

The CTM product suite will enable secure device–to–device communication, dynamic third party connection trust negotiations, support compliance with NERC/FERC, NIST, and other applicable standards, and allow centralized management of control system cryptographic material.

User and Environment Characteristics

Operating knowledge of cryptographic technologies and functions is required to operate the system securely. Proper installation, configuration, and operation of security systems are critical to their ability to perform their security task. Even the most secure systems can be compromised if they are not configured and maintained properly.

See the use cases in Appendix A for a detailed example of how the CTM product suite will be used.

Product Perspective

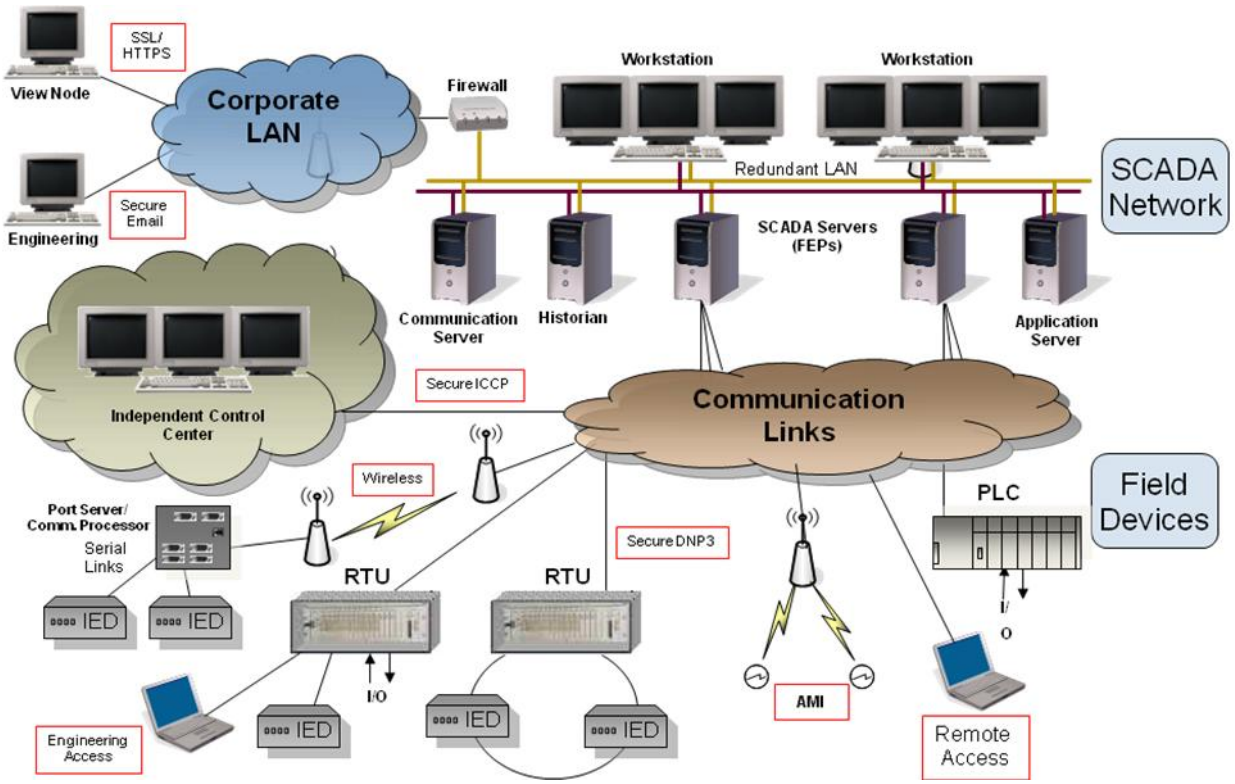

Figure 1 – Control System Network Security Connections

General Constraints

Assumptions and Dependencies

Assumptions

The CTM task will focus on communication within the Control System network. It will not directly target applications used for enterprise communication.

Dependencies

As the PNNL Control Systems Security Research and Development Program progresses, the dependencies and interdependencies across the different projects will become evident.

To date, one of the major dependencies identified is the Secure Data Transfer (SDT) project – Cryptographic Trust project dyadic interaction and reinforcement. This aspect of the two projects will be further analyzed and assessed as part of the projects' conduct.

The control system security environment is in a rapid state of evolution. Several standardization efforts are under way to try and define the landscape of the future control system. NIST, NERC, ISA, IEEE and other standards organizations are all working on control system standards that could be relevant

to this project. In particular the NIST Smart Grid Interoperability Framework will contain the standards most heavily influential to the Smart Grid development in the United States. Therefore, the PNNL NSTB technical team will maintain awareness of NIST and other industry standard activities. As the new standards are released, this RS will be updated to align with industry accepted standards.

1.0 Functional Requirements

This section specifies what the CTM product suite must be able to perform – the fundamental actions that transform inputs into the project's desired outputs or capabilities.

1.1 Requirements

1.1.1 Must provide functionality to negotiate trust with external entities to; enable external entities, down to the granularity of device and/or person, and securely communicate with internal systems and devices by exchanging the necessary session key material upon verification of external parties meeting industry/enterprise specific requirements. The verification process will check, at a minimum, the validity of cryptographic material in regards to employment actions, expiration, and revocation.

1.1.2 Must automate the key management of device-to-device communication. Must provide manual key management to support legacy equipment that does not support the CTM.

1.1.3 Must provide a centralized location to manage cryptographic material and trust relationships.

1.1.4 Must provide secure storage for cryptographic material via encryption and role based access.

1.1.5 Must securely generate cryptographic material by meeting all applicable NIST standards.

1.1.6 Must alert when cryptographic material expires and new cryptographic material has not been distributed to all affected devices and/or people. For manually managed cryptographic material, the CTM must also alert a user configurable percentage of the lifespan of the cryptographic material.

1.1.7 Must provide the ability to revoke cryptographic material.

1.1.8 Must archive old cryptographic material for user configured time lengths and allow for retrieval.

1.1.9 Must support device registration, both manually and automatically, to the CTM.

1.1.10 Must support the configuration of priority of cryptographic material for degradation of failure. If the system begins to fail or is unable to perform all of the tasks in a needed time frame, it will complete the functions involving the cryptographic material with the highest priority first.

1.1.11 Must support back-up of cryptographic material and configuration information capabilities.

2.0 External Interface / Usability Requirements

This section specifies the characteristics of interfaces between the CTM product suite and other systems or components and human users, hardware, software, objects or business rules. Usability requirements specify factors affecting how easily users can learn to operate the CTM system and/or components, prepare its inputs, and interpret its outputs.

2.1 User Interface Requirements

2.1.1 Must support separation of roles and role based access for access to cryptographic material, administrative configuration functionality, and access to reports.

2.1.2 Must provide a web-based graphical user interface for configuration and management of key policies, device cryptographic material, external party negotiation policies, report information, cryptographic material retrieval, and key revocation.

2.1.3 Must utilize role-based access control for cryptographic material retrieval, configuration, and report access based on organization prescribed role.

2.1.4 Must provide capability to construct a report for auditors that includes information such as key metadata (lifecycle information, bit strength, and devices utilizing) and policy violations (keys expired without distribution of new keys, systems requests for inappropriate cryptographic material, and request for communications between devices/people without proper privileges).

2.1.5 Must provide support for forensic analysis by maintaining a history of which devices have cryptographic material, when cryptographic material was distributed, and which devices/people requested to communicate and to which device. The CTM must provide functionality in the user interface to retrieve the forensic information based on user criteria (i.e., which device, time frame, and key material they are interested in).

2.1.6 Must provide a user configurable alarming mechanism to alert user to expired cryptographic material, unknown devices, failed trust negotiations, or other erroneous events.

2.1.7 Must provide a manual cryptographic management interface to support legacy devices that are not compatible with the CTM. This interface should provide the capability to create key material and associate it with a device.

2.1.8 Must provide a report system to report the cryptographic status (what devices are they communicating with and cryptographic material lifecycle metadata) of the all devices and systems managed and any system or cryptograph errors that have occurred. The report system must provide audit, forensic, system health, and system performance views.

Hardware Interface Requirements

2.1.9 Must support hardware interfaces for the use of hardware tokens or LUNA modules for the identification of the key authority and also for the manual distribution of key material.

2.2 Communications Interface Requirements

2.2.1 CTM must communicate directly via a standard protocol with devices or vendor-specific product configuration software for key management functions (key requests, communication requests, and key expiration/revocation).

2.2.2 Must interface with CTM systems at other utilities or cryptographic trust management services for trust negotiation.

2.2.3 In addition to offering custom identity management capabilities, CTM will be able to utilize existing key management infrastructure (at a minimum the Entrust PKI) to access identity cryptographic material and metadata.

2.3 Usability Requirements

2.3.1 Must operate in an automated fashion with compatible devices, after initial configuration, to maintain the lifecycle of cryptographic material (key update, distribution, request, expiration, and revocation).

2.3.2 Both user and device cryptographic material can be managed by CTM.

3.0 Design Constraints

Design constraints are requirements or choices that set boundaries on the CTM design solutions possible for implementing other requirements.

Requirements

3.1.1 CTM shall NOT be limited to a specific transmission medium.

3.1.2 CTM shall NOT be limited to a single platform or vendor.

3.1.3 CTM shall NOT be limited to a specific cryptographic method / technique.

3.1.4 CTM does NOT duplicate existing commercial solutions.

3.1.5 CTM is NOT industry/sector specific.

Standards Compliance

3.1.6 CTM shall be designed to meet FIPS 140-2, 180-3, 186-3 and other applicable standards. The standards identified by the NIST Interoperability Framework for the Smart Grid will be reviewed and addressed by the CTM design. However, formal validation against these standards is out of scope.

3.1.7 CTM shall be designed to meet industry standard entropy requirements. IETF RFC 4086 shall be referenced during design and only FIPS approved pseudo-random number generators will be used. NIST 800-22 and FIPS 140-2 statistical tests shall be utilized to ensure entropy levels are met.

Hardware Limitations

3.1.8 Hardware and key storage solutions must support key history for at least three years (NERC CIP-002-01 D.1.3).

Other Limitations

3.1.9 CTM must scale to support as low as 10+ up to 100,000,000 entities.

3.1.10 Asymmetric keys shall be supported for user identity. Symmetric keys shall be supported for device identity. Asymmetric keys shall also be supported for device identity for devices that have adequate resources.

4.0 Performance Requirements

This section imposes performance requirements (such as speed or accuracy) as a functional requirement or set of functional requirements of the CTM product suite.

Requirements

4.1.1 CTM does not adversely impact control system operation.

4.1.2 The CTM product suite will be resilient and hardened, with an architecture that supports high availability and fails gracefully.

4.1.3 The CTM product suite will be scalable and will have low enough overhead so that it can be transported over low bandwidth links.

5.0 Reliability Requirements

This section specifies the reliability requirements of the CTM product suite in performing its required functions under stated conditions for a specified time period.

Requirements

5.1.1 Must be reliable at least 99.5%.

5.1.2 Must meet or exceed the control system's reliability requirement.

5.1.3 CTM must persevere in the event of a reliability event (such as an attack), alert the user of the issue, and prioritize system, devices, and services according to configuration priorities.

6.0 Security Requirements

This section specifies needs for protecting the CTM system or components from accidental or malicious access, use, modification, destruction, or disclosure.

Requirements

6.1.1 CTM securely and confidentially performs all key management functions.

6.1.2 Key material is securely stored according to best practice methodology.

6.1.3 CTM will only allow a minimal attack surface through available port reduction.

6.1.4 CTM correctly performs all cryptographic functions.

6.1.5 FIPS approved cryptographic algorithms will be utilized by CTM to develop keys, protect keys, and communicate through all external interfaces.

6.1.6 CTM will ensure unique keys are utilized across systems and networks.

7.0 Availability Requirements

This section specifies factors affecting the likelihood that the CTM system or components will be operational and accessible when required for use.

Requirements

7.1.1 Must be operational and accessible at least 99.5%.

7.1.2 Must meet or exceed the control system's availability requirement.

7.1.3 Availability will not be adversely affected by upgrades or updates via principle of redundancy OR software assisted transfer and change capabilities.

7.1.4 Must provide, as applicable, mechanisms and procedures for failover to redundant site.

8.0 Portability Requirements

Portability requirements specify factors affecting how easily the CTM system or components can be transferred from one hardware or software to another.

Requirements

8.1.1 CTM is not application, device, or vendor specific.

8.1.2 CTM should be designed so that it is not operating system dependent.

9.0 Supportability Requirements

This section details supportability requirements including requirements affecting how easily the CTM product suite and its components can be maintained to meet original requirements or extended to meet modified requirements.

Requirements

9.1.1 The CTM solution shall provide online help and guidance to assist in proper configuration and maintenance.

10.0 Other Requirements

This section details other requirements, including special requirements that do not fit into previous categories.

Requirements

Appendices

Appendix	Information
A: Use Cases	Description of how end users will possibly use the CTM product suite
B: Definitions, Acronyms, and Abbreviations	A glossary of terms that appear in the RS
C: NSTB Advisory Board/PNNL Technical Members	Roster of industry advisors and technical experts
D: References and Resources	A list of the documents referenced in the RS and where to find them.

Appendix A. Use Cases

A.1. Request Key Material

Goal

The key material requested is created, stored, and delivered to the requesting actor.

Summary

This use case describes an automated method for applications, systems, or devices to retrieve key material from system.

Actors

Application, System, or Device

Preconditions

The actor must communicate in a protocol that the system supports to enable the requesting and delivery of the key material.

Triggers

The actor sends a request for key material to the system.

Event Flow

1. Actor establishes secure connection with trust system.
2. Actor sends key material request to trust system. The request includes what type of key material, how much key material, and other necessary/vital information.
3. Trust system generates key material.
4. Trust system stores key material and metadata (who key material is for and life time of key material).
5. Trust system transmits key material to actor.

Implementation Examples

- SSCP device requesting Master keys or pre-shared key list
- Zigbee gateway requesting link and application keys for new joining device.

A.2. Request Communication Key Goal

Keys enabling two actors to communicate are distributed to the two actors.

Summary

This use case describes an automated method for an actor to request a key that enables it to communicate with another actor. This key may already be created and used by the second actor or may need to be created and distributed to both devices.

Actors

Application, System, or Device

Application, System, or Device

Preconditions

The actors must communicate in a protocol that the system supports to enable the requesting and delivery of the key material.

Triggers

The actor sends a request for a key to communicate with another actor.

Event Flow

1. Actor sends request to trust system for key material for communication with another actor. The request includes information identifying with whom the actor will communicate.
2. Trust system checks trust relationships to see if it will allow communication between actors.
3. Trust system sends key material to requesting actor.
4. Trust system sends key material to second actor. (Optional, depending on type of cryptographic system used by second actor).

Implementation Examples

- New network sensor requesting key to communicate with visualization tool.
- SSCP slave device requests key for communication with Master SSCP device.

A.3. Expire Key Material

Goal

The key that has expired is stopped from being used by the actor, and a new key is distributed to the actor.

Summary

The trust management system is responsible for key material and now must enforce key expiration. The system must notify and rekey the actor when their key material expires. (Maybe add the use case for early notifications, so the actor can rekey when it is convenient for them.)

Actors

Application, System, or Device

Preconditions

The actor must communicate in a protocol that the system supports to enable the requesting and delivery of the key material.

The actor must have previously requested key material from the trust management system.

Triggers

Time out for the key material.

Event Flow

1. Key material life time expires.
2. Trust system creates secure connection with actor.
3. Trust system notifies actor of key expire.
4. Actor starts request key material use case (optional).

Implementation Examples

- Certificate expires.
- SSCP Master keys expire.
- ISA100.11a session keys expire.

A.4. Negotiate Trust Session

Goal

An actor from a third party is allowed to communicate on the system, and necessary communication keys are distributed by communication with the third party's trust system.

Summary

Third party actors may need access to the environment being protected by the trust management system. This use case describes the process of negotiating the trust between the parties and distributing the necessary key material to the third party / visiting actor to allow this actor to perform work.

Actors

Application, System, or Device
Third Party Trust Management System

Preconditions

None

Triggers

Request by third party actor to communicate with actor managed by the trust system.

Event Flow

1. Third party actor requests access to actor managed by trust system. As part of the request, the third party actor provides credentials (i.e., identifier, authentication information, and third party trust management system information).

2. Trust system checks trust relationships and trust stance.

3. If relationship and stance checks are OK, trust system communicates with third party trust management system to authenticate and define access rights of third party actor.

4. Trust system sends necessary key material to third party actor to access local actor.

5. If necessary, trust system sends key material to local actor to allow communication.

Implementation Examples

- Mobile Plug-in Hybrid Electric Vehicle infrastructure.

- Integrator/Vendor access to utility equipment.

A.5. Revoke Key Material

Goal

The key material used by an actor or actors is expired.

Summary

The trust management system is responsible for managing the key material for the actors that use it. At some point, the key material used by an actor or actors becomes un-trusted due to an event. This use case describes the process a user would go through to revoke a key.

Actors

User
Application, System, or Device (maybe not need)

Preconditions

None

Triggers

User revokes key.

Event Flow

1. User or actor invokes process to revoke key material (GUI, API).
2. Trust system communicates with all actors using key material that the key has been revoked.
3. Trust system archives key material and metadata that has been revoked.

Implementation Examples

- Employee termination.
- Compromised system.

A.6. Provision System

Goal

The trust management system is configured and in an operational state ready to perform tasks.

Summary

The trust management system will require some initial configuration before it is operational. This use case defines the process to perform the initial configuration of the system.

Actors

User

Preconditions

None

Triggers

User manually triggers this use case.

Event Flow

1. User installs/creates initial key material (root certificate).

A.7. Configure Trust Relationship

Goal

A relationship is enabled between this trust management system and a third party trust management system.

Summary

The trust system is supposed to manage the trust for the entity. As part of this trust, it is expected that external parties will require access the entities actors. This use case describes the process to configure trust relationships with third parties to enable automatic access for third party actors to communicate with the entity's actors.

Actors

User

Preconditions

None

Triggers

User manually triggers this use case.

Event Flow

1. User configures trust relationship (GUI, API).
    a. Third party information.
    b. Access allowed for each configured trust stance.

Implementation Examples

- Integrator/Vendor access to utility equipment.

A.8. Retrieve Key Information

Goal

User extracts key material or metadata from archived data.

Summary

The trust management system will be required to archive and store key material for auditing and forensic purposes. This use case describes the process the user takes to retrieve current or archived key information from trust management system.

Actors

User

Preconditions

Key material must be archived before it can be retrieved.

Triggers

User requests key information.

Event Flow

1. User requests key information (GUI or API).
2. Trust system authenticates user for access privileges.
3. Trust system returns key information.

Implementation Examples

- Forensic investigation.
- Regulatory audit.

A.9. Manual Key Material Request

Goal

User installs key material for actor that cannot communicate with trust management system directly.

Summary

The trust management system must work with applications that were not developed to interface with it. This use case defines the process a user takes to use the trust management system with the external application.

Actors

User
Application, System, or Device

Preconditions

None

Triggers

User manually requests key material.

Event Flow

1. User requests key material (GUI or API).
    a. System identifier using key material.
    b. Type of key material to be created.
2. Trust system authenticates user.
3. Trust system generates key material and stores it.
4. Trust system delivers key material to user.
5. User installs key material into actor.

Implementation Examples

- Any current system that was not developed to operate with trust system.

Appendix B: Definitions, Acronyms, and Abbreviations

Some of the following definitions are taken or adapted from IEEE Std 610.12-1990 (IEEE 1993a) and IEEE Std 830-1984 (IEEE 1993b).

AGA — American Gas Association

availability — the degree to which a system or component is operational and accessible when required for use. Often expressed as a probability [IEEE Std 610.12-1990].

CTM — Cryptographic Trust Management

component — one of the parts that make up a *system.* A component may be hardware or software and may be subdivided into other units or components [IEEE Std 610.12-1990]. Note: For the purpose of this **specification**, the term "component" will be used in preference to the terms "module" and "unit."

DOE — Department of Energy

EIOC — Electric Infrastructure Operations Center

extendibility — the ease with which a system or component can be modified to increase its storage or functional capacity [**IEEE** Std 610.12-1990] (synonyms: extensibility; expandability).

FERC — Federal Energy Regulatory Commission

FIPS — Federal Information Processing Standard

functional requirement — a requirement that specifies a function that a system or system component must be able to perform [IEEE Std 610.12-1990]. In this requirements specification, functional requirements **specify** how the inputs to the software product should be transformed into outputs [IEEE Std 830-1984].

interface requirement — a requirement that specifies an external item with which a system or system component must **interact** or that sets forth constraints on formats, timing, or other factors caused by such an interaction [IEEE Std 610.12-1990].

LUNA modules — a type of secure cryptoprocessor targeted at managing digital keys for server applications.

maintainability — the ease with which a software system or component can be modified to correct faults, improve **performance** or other attributes, or adapt to a changed environment [IEEE Std 610.12-1990] (contrast with *extendibility*).

module — see *component*.

NERC — North American Electric Reliability Corporation

NIST — National Institute of Standards and Technology

NSTB — National Transportation Safety Board

performance— the **degree** to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage [IEEE Std 610.12-1990] (contrast with *reliability*).

performance requirement — a requirement that imposes conditions on a functional requirement; for example, a requirement that **specifies** the speed, accuracy, or memory usage with which a given function must be performed [IEEE Std 610.12-1990] or a static numerical requirement such as the number of simultaneous users to be supported or the number of files and records to be handled [IEEE Std 830-1984].

PNNL — Pacific Northwest National Laboratory

portability — the ease with which a system or component can be transferred from one hardware or software environment to another [IEEE Std 610.12-1990] (synonym: transportability).

product — (for this document) a system or component–along with any necessary data and documentation–for which **requirements** are specified in a *requirements specification*.

reliability — the ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE Std 610.12-1990] (contrast with *performance*).

requirement — (1) a condition or capability needed by a customer to solve a problem or achieve an objective; (2) a condition or **capability** that must be met or possessed by a *system* or *component* to satisfy a contract, standard, *specification*, or other formally imposed document; (3) a documented representation of a condition or capability as in (1) or (2) [adapted from IEEE Std 610.12-1990].

requirements specification (RS) — a document of the essential *requirements* (functions, performance, design constraints, and attributes) of the software and/or hardware and their external interfaces [adapted from IEEE Std 610.12-1990].

RS — *requirements specification*.

SDT — Secure Data Transfer

SSCP — Secure SCADA Communication Protocol.

system — a collection of components related in such a way as to produce a result greater than what their parts, separately, could produce.

unit — see *component*.

usability — the ease with **which** a user can learn to operate, prepare inputs for, and interpret outputs of a system or component [IEEE Std 610.12-1990].

Appendix C. NSTB Advisory Board and Technical Team Members

NSTB Advisory Board	
Member	**Organization**
Dave Batz	Alliant Energy
Dave Scheulen	BP
Page Clark	El Paso Corporation
Steve Elwart	Ergon Refining, Inc.
Eric Fletcher	NiSource
Tom Flowers	Flowers Control Center Solutions
Ed Goff	Progress Energy
Morgan Henri	Alyeska Pipeline, Inc.
Dave Norton	Entergy Corporation
PNNL Technical Team Members	
Bryan McMillian	Mark Hadley
Anne Ouderkirk	John Burnette
Thomas Edgar	Sean Zabriskie
Surya Singh	Samuel Clements
Bill Flynt	Wendy Maiden
Ben Garza	

Appendix D. References and Resources

Pacific Northwest National Laboratory. December 4, 2008. *NSTB Advisory Board: Kick-Off NSTB Advisory Board Meeting.* PowerPoint presentation, Battelle, Washington, D.C. *(Unpublished report: NOT permitted in publicly available documents)*

Pacific Northwest National Laboratory. 2001. *Software Systems Engineering Process Guide*. Available at http://ssep.pnl.gov/. Pacific Northwest National Laboratory, Richland, Washington.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov