



FINAL REPORT

Closed Restricted Network PKI Certificate Authority for Facility- related Control Systems

Ryan McKinley
Aura Lee Keating
Peter Curtiss
C2 Company a PrimeKey Company

December 2021

This report was prepared under contract to the Department of Defense Environmental Security Technology Certification Program (ESTCP). The publication of this report does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official policy or position of the Department of Defense. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Department of Defense.

REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY)

14-02-2022

2. REPORT TYPE

ESTCP Final Report

3. DATES COVERED (From - To)

9/30/2020 - 9/30/2022

4. TITLE AND SUBTITLE

Closed Restricted Network PKI Certificate Authority for Facility-related Control Systems

5a. CONTRACT NUMBER

20-C-0071

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

Ryan McKinley
Aura Lee Keating
Peter Curtiss

5d. PROJECT NUMBER

EW20-5299

5e. TASK NUMBER

N/A

5f. WORK UNIT NUMBER

N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

PrimeKey: S&C Electric:
951 Mariners Island Blvd, 6601 N. Ridge Blvd.
#210 Chicago, IL 60626-3997
San Mateo, CA 94404

8. PERFORMING ORGANIZATION REPORT NUMBER

EW20-5299

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Environmental Security Technology Certification Program
4800 Mark Center Drive, Suite
16F16, Alexandria, VA 22350-3605

10. SPONSOR/MONITOR'S ACRONYM(S)

ESTCP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

EW20-5299

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Public Key Infrastructure (PKI) security is not possible in air-gapped networks isolated from PKI servers, and as air-gapped systems and networks increase in size and complexity, additional protections are necessary to secure them. Not only is end-to-end, device-to-device authentication needed, but also the means to encrypt the open communication protocols control systems commonly use. The objective of this Proof-of-Concept project is to demonstrate a repeatable, quick-to-deploy, and automated Certificate Authority (CA) solution to bring enhanced security of PKI capabilities to Closed Restricted Network (CRN) control systems, such as those commonly used for DoD Control Systems, that will provide: (1) Resiliency of Facility-related Control System (FRCS) networks through stronger Confidentiality, Integrity, & Availability (CIA) of files and connections, (2) Compliance of cybersecurity requirements for control systems, and (3) Applicability beyond FRCS.

15. SUBJECT TERMS

Closed Restricted Network, PKI Certificate Authority, Facility-related Control Systems

16. SECURITY CLASSIFICATION OF:

Unclassified (U)

17. LIMITATION OF ABSTRACT

UU

18. NUMBER OF PAGES

76

19a. NAME OF RESPONSIBLE PERSON

Ryan McKinley

19b. TELEPHONE NUMBER (include area code)

916-768-9422

FINAL REPORT

Project: EW20-5299

TABLE OF CONTENTS

	Page
ABSTRACT	X
EXECUTIVE SUMMARY	ES-1
1.0 INTRODUCTION	1
1.1 BACKGROUND	2
1.2 OBJECTIVES OF THE DEMONSTRATION.....	3
1.3 REGULATORY DRIVERS	3
2.0 TECHNOLOGY DESCRIPTION	5
2.1 TECHNOLOGY OVERVIEW	5
2.1.1 PrimeKey EJBCA	6
2.1.2 GridMaster® Intelligent Power Controller	9
2.1.3 HMI.....	10
2.1.4 Syslog Server	11
2.1.5 Woodward LS5 and Secure Endpoints	11
2.1.6 Simulation Computer	12
2.2 TECHNOLOGY DEVELOPMENT.....	12
2.2.1 Establish Environment for Testing and Development	13
2.2.2 Initial Testing and Development.....	13
2.3 CRN EJBCA ADVANTAGES AND LIMITATIONS	16
2.3.1 Alternative Technologies	18
3.0 PERFORMANCE OBJECTIVES	20
3.1 PERFORMANCE OBJECTIVES DESCRIPTIONS	20
3.1.1 Quantitative Performance Objectives Descriptions	20
3.1.2 Qualitative Performance Objectives Descriptions	22
4.0 FACILITY/SITE DESCRIPTION.....	23
5.0 TEST DESIGN & DEMONSTRATION.....	24
5.1 CONCEPTUAL TEST DESIGN.....	24
5.1.1 Demonstration Test Phases	25
5.2 BASELINE CHARACTERIZATION.....	28
5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS	28
CRN PKI Demonstration Network.....	29
5.3.1 EJBCA Integration.....	29
5.3.2 GridMaster® Microgrid Control System	30
5.3.3 DER/Secure Endpoints	31
5.3.4 Syslog Server	31

TABLE OF CONTENTS (Continued)

	Page
5.3.5 CHIL Network	31
5.4 OPERATIONAL TESTING	32
6.0 PERFORMANCE ASSESSMENT	34
7.0 COST ASSESSMENT	35
7.1 COSTS ASSOCIATED WITH ESTABLISHING PKI RESOURCES FOR THE CRN	35
7.2 COSTS ASSOCIATED WITH IMPLEMENTING PKI CAPABILITY ON END DEVICES ON THE CRN	35
7.2.1 Device Type	35
7.2.2 Device Type Uniformity	36
7.2.3 Level of Automation	36
7.2.4 Level of PKI Expertise.....	36
7.3 COST MODEL	36
7.3.1 EJBCA PKI Software Appliance	37
7.3.2 GridMaster IPC – Representative FRCS	37
7.3.3 Secure Endpoint.....	37
7.3.4 Installation Costs.....	38
7.3.5 Maintenance.....	38
7.3.6 Hardware Lifetime	38
7.3.7 Operator Training.....	38
7.4 COST DRIVERS	39
7.5 COST ANALYSIS AND COMPARISON.....	39
8.0 IMPLEMENTATION CONSIDERATIONS	40
8.1 END DEVICE PKI CAPABILITIES	40
8.2 PROTECTING CRITICAL OPERATIONS	41
8.3 PKI AUDITING.....	41
8.4 CERTIFICATE VALIDATION AND EXPIRATION OPTIONS.....	42
8.4.1 Automatic Certificate Revocation.....	42
8.4.2 Revocation Checking	42
8.5 KEY STORAGE.....	43
8.6 ACCURATE TIME SOURCE	43
8.7 UI FOR END DEVICES	44
9.0 REFERENCES	45
APPENDIX A CLIENT CONSIDERATIONS.....	A-1
A.1 CLIENT-SIDE SCRIPTING	A-1
A.1.1 Utility Used for Client-Side PKI Functions at NREL Demonstration	A-2
A.2 SECURE ENDPOINTS	A-5
A.3 OTHER USE CASES	A-6
A.3.1 Signing Site-Created Documents, Files and Recovery Images.....	A-6

TABLE OF CONTENTS (Continued)

	Page
A.3.2 NTP	A-6
A.3.3 User Authentication	A-7
APPENDIX B POINTS OF CONTACT.....	B-1
APPENDIX C PRIMEKEY EJBICA HARDWARE APPLIANCE.....	C-1
APPENDIX D PKI AUTHENTICATION STIG REQUIREMENTS	D-1

LIST OF FIGURES

	Page
Figure 1. Using Local PKI to Secure a CRN.....	1
Figure 2. Conceptual Diagram of Full Solution	5
Figure 3. PrimeKey EJBCA Architecture.....	7
Figure 4. EJBCA Model View Controller Design.....	8
Figure 5. EST Protocol between GridMaster IPC and EJBCA	9
Figure 6. S&C GridMaster IPC Microgrid Controller.....	10
Figure 7. EJBCA running as a VM on a VirtualBox Host	14
Figure 8. Code Snippet Showing CURL Command with Variables	14
Figure 9. Example of Syslog-ng Config File Showing PKI Filesystem Locations	15
Figure 10. Local Configuration Utility on Client Devices	15
Figure 11. Demonstration at NREL	25
Figure 12. Testbed Setup	26
Figure 13. Demonstration at NREL	27
Figure 14. Demonstration at NREL	28
Figure 15. Conceptual Setup and Connectivity of the CRN EJBCA CHIL	29
Figure 16. Typical GridMaster System HMI Graphical User Interface	31
Figure 17. Initial Configuration Menu.....	A-3
Figure 18. EST Client Settings	A-3
Figure 19. Utility Provides a Means of Entering the Initial Enrollment Credential	A-4
Figure 20. Utility Indicates Success or Failure during Enrollment/Re-Enrollment	A-4
Figure 21. Sample Logs for PKI Activities through the Client-Side Utility.	A-5
Figure 22. Sample EJBCA Detailed Audit Logging.....	A-5
Figure 23. Locally Generated Log Entry Showing a Certificate Validation Issue	A-5
Figure 24. Secure Endpoints Use Case.....	A-6

LIST OF TABLES

	Page
Table 1. Performance Objectives	3
Table 2. Performance Objectives	20
Table 3. Cost Model for a CRN PKI CA for Facility-related Control Systems	37
Table 4. PKI-Related Capabilities	40
Table 5. Local Functionality for PKI Participation.....	A-1
Table 6. Points of Contact.....	B-1

ACRONYMS AND ABBREVIATIONS

AD	Active Directory
AIA	Authority Information Access
API	Application Programming Interface
CA	Certificate Authority
CCI	Control Correlation Identifier
CDP	CRL Distribution Points
CHIL	Controller Hardware in the Loop
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CRN	Closed Restricted Network
CSR	Certificate Service Request
CURL	Client Uniform Resource Locator
DB	Database
DCM	Distributed Communication Management
DER	Distributed Energy Resource
DISA	Defense Information Systems Agency
DNP	Distributed Network Protocol
DNS	Domain Name System
DoD	Department of Defense
EAR	Enterprise Archive
ECC	Elliptic-curve cryptography
EJB	Enterprise Java Beans
EJBCA	Enterprise Java Beans Certificate Authority
ESIF	Energy Systems Integration Facility
EST	Enrollment over Secure Transport
ESTCP	Environmental Security Technology Certification Program
FRCS	Facility-related Control Systems
GenSet	Generator Set
GPS	Global Positioning System
GUI	Graphical User Interface
HMI	Human Machine Interface
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
IED	Intelligent Electronic Device
iOS	Internetwork Operating System (Cisco)
IP	Internet Protocol

IPC	Intelligent Power Controller
IPV	Internet Protocol Version
IT	Information Technology
JDK	Java Developer Kit
MAC	Media Access Control
MitM	Man in the Middle
NDES	Network Device Enrollment Service
NIST	National Institute of Standards and Technology
NMAP	Network Mapper
NREL	National Renewable Energy Laboratory
NSA	National Security Agency
NTP	Network Time Protocol
OCSF	Online Certificate Status Protocol
OT	Operational Technology
OVA	Open Virtual Appliance
PKI	Public Key Infrastructure
PKCS	Public-Key Cryptography Standard
PKCS#11	Public-Key Cryptography Standard #11
PoC	Proof of Concept
RA	Registration Authority
RMF	Risk Management Framework
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman
SBC	Single Board Computer
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SFP	Security Foundation Platform
SIL	Software in the Loop
SMA	SubMiniature version A
SSH	Secure Shell
STIG	Security Technical Implementation Guide
SRG	Security Requirements Guide
TLS	Transport Layer Security
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guidance Specification
UI	User Interface

VA	Validation Authority
VDC	Volts of Direct Current
VM	Virtual Machine
WAR	Web Archive
XML	Extensible Markup Language
YAML	Yet Another Markup Language

ACKNOWLEDGMENTS

The following individuals and organizations contributed to the demonstration project and the generation of the final report:

PrimeKey	S&C Electric	National Renewable Energy Laboratory
Ryan McKinley	Aura Lee Keating	Brian Miller
Linda Gopal	Christopher Rowland	John Nangle
Jeff Brooks	Chad Douglas	Richard Macwan
Margaret Doty	Peter Curtiss	Joshua Rivera
	Michael Pinkston	

ABSTRACT

INTRODUCTION AND OBJECTIVES

Public Key Infrastructure (PKI) security is not possible in air-gapped networks isolated from PKI servers, and as air-gapped systems and networks increase in size and complexity, additional protections are necessary to secure them. End-to-end encryption and device-to-device authentication are lacking in many DoD Facility-Related Control Systems (FRCS). The objective of this Proof-of-Concept project is to demonstrate an automated certificate management solution to bring the enhanced security of a PKI Certificate Authority (CA) to a control system commonly operating in Closed Restricted Networks (CRNs) in the DoD – a “CRN CA.”

Project objectives met demonstrated a low-cost solution to add “internal PKI” security capabilities within closed environments where interconnections with external PKI resources are not feasible or would unduly increase the attack surface of the FRCS. The demonstrated solution supported objectives for simple, quick, low-cost implementation, enhanced security, and extension of the encryption footprint to unsecured endpoints (e.g., Distributed Energy Resources (DERs)).

TECHNOLOGY DESCRIPTION

The demonstrated CA CRN solution integrates PrimeKey’s Enterprise Java Bean Certificate Authority (EJBCA) PKI Software and S&C Electric’s GridMaster[®] Microgrid Control System as the representative FRCS. EJBCA provided certificates to end-devices and validation services. S&C provided a network of equipment common in microgrid CRNs - 2 microgrid controllers, an HMI for interfacing with the controllers, a Linux syslog server, a Woodward LS-5 to represent a typical DER, and S&C’s GridSim[™] to generate microgrid traffic. To demonstrate a method of authenticating and securing communications to a PKI-incapable DER (i.e., the LS-5), “Secure Endpoints” with EST clients were added to the CRN CA solution’s architecture.

PERFORMANCE AND COST ASSESSMENT

Project objectives were met proving the utility and feasibility of adding an internal PKI to a closed network to secure communications between a diverse group of equipment administered by personnel unfamiliar with PKI concepts. The minimal cost of setting up a CRN CA will need to be scaled based on cost drivers including the number of PKI client devices and implementation methods per device type, and the targeted level of PKI implementation and automation.

IMPLEMENTATION CONSIDERATIONS

Integration of PKI is facilitated by commercially available EJBCA software, so most implementation considerations fall to the PKI capabilities of the client endpoints, including operational impacts with increased bandwidth and processing power usage, auditing configuration and monitoring for PKI activities, key storage, accurate time sources, and certificate validation and revocation options.

PUBLICATIONS

Concluding documentation generated during this project includes the Final Report, slides for the 2021 ESTCP Symposium, and project Fact Sheet, and Technology Transition Plan.

EXECUTIVE SUMMARY

INTRODUCTION

The technology demonstrated at the National Renewable Energy Laboratory (NREL) in June 2021 is a locally contained PKI (Public Key Infrastructure) in a Closed Restricted Network (CRN) to address the need for strong authentication and encryption among Facility-related Control System (FRCS) devices. This methodology allows for (1) strong security controls within the network while (2) allowing the network to remain isolated at the perimeter.

The demonstrated solution is a PKI platform embedded in an Intelligent Electronic Device (IED) using the PrimeKey Enterprise Java Beans Certificate Authority (EJBCA) software with S&C's GridMaster® Microgrid Control System. The solution addresses hardware limitations of FRCS equipment to support cybersecurity functions, low-latency network environments, and preserving the security posture through rapid configuration changes.

OBJECTIVES

The overall objective of the project was to demonstrate a low-cost solution to add the security capabilities of PKI in CRN environments that resolves the dilemma of either 1) having no access to a CA server (and no PKI capabilities), or 2) establishing interconnections that may increase the attack surface of the otherwise closed network.

Supporting objectives included:

- Quick and easy deployment of the CRN PKI solution
- Low-cost implementation
- Enhanced security
- Extension of encrypted communications to Distributed Energy Resources (DERs)

TECHNOLOGY DESCRIPTION

The demonstrated technology included the following components:

PrimeKey EJBCA - a commercial PKI solution available from PrimeKey. It is a scalable Java-based Certificate Authority that can be used to issue and manage certificates (CA functions), as well as provide services such as OCSP and CRL distribution during regular operations. The EJBCA provides a secure web-based front end which allows for straightforward and user-friendly configuration and management. For the purposes of the demonstration, the EJBCA was installed as a virtual machine on a Windows 10 laptop hypervisor running Oracle VirtualBox. Once installed and configured, EJBCA provided all PKI infrastructure and functionality for the test network.

S&C GridMaster® Microgrid Control System – S&C's GridMaster Intelligent Power Controllers (IPCs) automate control of grid assets to maintain stable, reliable, and economic microgrids. For the demonstration, two IPCs were programmed to utilize PKI services.

A third IPC, identical in all software aspects, but not provisioned with certificates from the local CA, was used for security testing as a ‘rogue’ device. An HMI computer and Syslog Server were also included as end devices in the demonstrated microgrid control system.

Secure Endpoints – specially programmed single board computers with serial ports obtained certificates through EST allowing for strong device authentication and encryption between the endpoints. Serial data was securely sent across a TLS connection, confining the use of plaintext protocols to a short distance between the DER and the collocated Secure Endpoint.

DER – a Woodward LS5 represented a DER that cannot be configured with the ability to use EST to obtain certificates or establish TLS connections. It offers a serial connection only, and its underlying operating system is inaccessible to the end user.

S&C GridSim – a workstation set up with software-in-the-loop to generate operational traffic within the microgrid control system, such as inter-controller communications, webpage content, and generating traffic on the network.

PERFORMANCE ASSESSMENT

The proposed performance objectives were met (see Table 1). The incorporation of PKI was shown to enhance security in that protocols were encrypted, endpoints were authenticated before making connections, and attempts to insert rogue devices were unsuccessful. Deployment activities (such as configuration of the EJBCA) were accomplished within the expected timeline through streamlining of configuration and deployment processes prior to the demonstration. Incorporation of PKI did not cause operational issues: the simulated and real devices continued to operate as expected.

Anecdotal observations were also made during the execution of the demonstration. Regarding the quickness and ease of EJBCA installation and setup, it’s more complicated to install the client needed on the end device (in this case the microgrid controller) than if using an Open Virtual Appliance (OVA) in hypervisor instance, but whatever system is running the virtual machine must still be hardened. Baseline EJBCA configurations for the CRN PKI consisting of the certificate profiles (restrict the key usage, key algorithms, and algorithm sizes the certificates commonly used on the CRN), CAs, and EJBCA EST settings can be maintained and imported using the EJBCA ConfigDump Tool. The EJBCA ConfigDump tool allows you to export and import configurations in a human-readable (YAML) format. With this import functionality, the complete EJBCA CRN PKI configuration can be imported into EJBCA to accelerate and facilitate the deployment. Security enhancements realized with EJBCA resolve several FRCS security requirement compliance and risk management gaps that have been long-standing issues (e.g., replaces long-life, self-signed certificates, ability to revoke certificates of decommissioned devices, encryption of geographically dispersed communication paths out to end devices (e.g., DERs)

Another key performance takeaway from the demonstration included S&C’s exploration of how to keep the system available when revoking a certificate. The first thought was to configure session breaks to force a revocation check, but new sessions are automatically established with the revoked certificate. A way to end sessions without rebooting that will force a revocation check of the expired or revoked certificate is needed. See 8.2 Protecting Critical Operations for more details.

Table 1. Performance Objectives

Performance Objective	Metric	Data Requirements	Success Criteria	Results
Quantitative Performance Objectives				
Quick EJBCA Deployment	Duration of EJBCA deployment activities	Representative control system administrator start-to-finish time for deployment activities	<60 minutes	Pass
Low Level of Effort for Realized Capabilities	Score of Ratio of adjustments to new capabilities	List of adjustments needed to stand up EJBCA with weighted levels of effort, list of additional capabilities with weighted values	Overall score indicates value of capabilities realized (benefit) outweighs the level of effort to implement (cost)	Pass
Enhanced Security	Additional cybersecurity requirement compliance enabled.	Baseline of PKI security requirements that are non-compliant without PKI capabilities	>90% compliance of PKI security control requirements dependent on access to a CA server	Pass
Qualitative Performance Objectives				
Ease of Use	Interviews of DoD components on ease of implementation	Interview results	Average responses indicate positive attitude or opinions on ease of use of the solution	Pass
Enhanced Security	Interviews of DoD components on enhanced security	Interview results	Average responses indicate positive attitude or opinions on enhanced security from deploying the solution	Pass

COST ASSESSMENT

Establishing PKI in a FRCS CRN has costs associated with 1) PKI resource integration for the site, and 2) PKI capability implementation on end devices. Costs are easily determined and controlled for PKI resource integration through use of a commercial PKI solution such as EJBCA. Implementation costs for end devices vary based on out-of-the-box capabilities, device types (e.g., standard IT, OS-based FRCS, firmware-only FRCS), device vendor/model uniformity, and the targeted level of automation for the PKI instance.

Another cost driver is the level of expertise of FRCS cybersecurity personnel. If outside support for engineering the environment for PKI and standing up the EJBCA is required, costs will be relatively higher and will vary based on the number of end devices in the environment, for example.

There are various cost elements that need to be considered for a CRN PKI. The EJBCA PKI Software Appliance and GridMaster IPC are the primary components, and their commercial costs are readily available. Other costs that will be required include installation & integration, support and maintenance, and training of operational and engineering staff. These other costs will vary, depending on the size of the deployment as well as the number of individuals to be trained.

IMPLEMENTATION CONSIDERATIONS

Integration of PKI is facilitated by the EJBCA which is a commercial product designed and supported for that purpose, so any implementation issues of the demonstrated technology will likely center around PKI capabilities on *end devices* (or lack thereof). It is necessary to first determine feasibility of interoperability and configuration methods for PKI on devices in the candidate network. For end devices that do not support PKI but need to have encrypted communications and/or be authenticated, use of collocated PKI-capable gateways or secure endpoints is recommended.

PKI-enabling or -enabled capabilities for end devices include:

- TLS support
- Local key and Certificate Service Request (CSR) generation
- EST (or equivalent) Client
- Renew certificates upon expiration
- Log and report certificate status
- Secure storage of the private key
- Reporting mechanism for validation errors
- Validation of peer certificates and trust chains (e.g., OCSP, CRL)

For some end devices, it may be enough to simply support TLS connections (i.e., use certificates provisioned by the EJBCA). For example, some Commercial Off-the-Shelf (COTS) devices can generate a CSR to use TLS, but the CSR must be manually transferred to the CA and signed. These devices are unable to automatically renew certificates and would require an administrator to replace expiring certificates via manual methods.

Additional considerations of PKI integration in FRCS environments include:

- Use of scripting or programming to automate PKI functions (e.g., certificate enrollment)
- Applying rate-limiting rules in a host-based firewall (e.g., to prevent denial of service due to invalid connection attempts)
- Managing persistent sessions to recognize revoked certificates
- Configuring audit functions to log PKI security events on the end device
- Certificate validation options (e.g., if current OCSP source or CRL is not available)
- Secure Private Key storage (e.g., software-based, hardware-based)

1.0 INTRODUCTION

Industrial networks are often treated as “walled gardens”, where devices described as “Operational Technology” (OT) reside within a protected enclave. Inside the enclave, the devices operate freely, unencumbered by the security controls which populate traditional IT networks. Security is provided only at the perimeter in this methodology (the “wall” around the “walled garden”), and hinges exclusively on the network being impenetrable to malicious actors.

There are legitimate reasons for treating industrial networks this way. These include:

1. Hardware limitations of OT devices, which are designed to execute specific tasks rapidly and reliably and cannot support security-oriented applications.
2. Network requirements for a low-latency network with sparse extraneous traffic.
3. Operational requirements that devices be rapidly replaced or reconfigured, often by operators whose skillset and priorities are different than those of a traditional IT administrator. Security controls tend to impede rapid reconfiguration and replacement.

However, it has become increasingly recognized that this “walled garden” approach is insufficient to address the increased sophistication, prevalence, and variety of cyber-attacks. To the extent possible, critical industrial networks need security controls *within* their boundaries, not just at the perimeter. This does not eliminate the need for protecting the perimeter of the network but is simply a recognition that internal security controls are necessary when they can be applied within the operational constraints identified above.

To address the requirements and apply defense in depth within the “walled garden,” an implementation of a *locally contained* PKI inside the constraints of a Closed Restricted Network, was evaluated to address the need for strong authentication and encryption among devices on a CRN. This methodology allows for 1) strong security controls within the network, while 2) allowing the network to remain isolated at the perimeter. The demonstrated solution is a PKI platform embedded in an Intelligent Electronic Device (IED) using PrimeKey’s Enterprise Java Beans Certificate Authority (EJBCA) software with S&C’s GridMaster® Microgrid Control System.

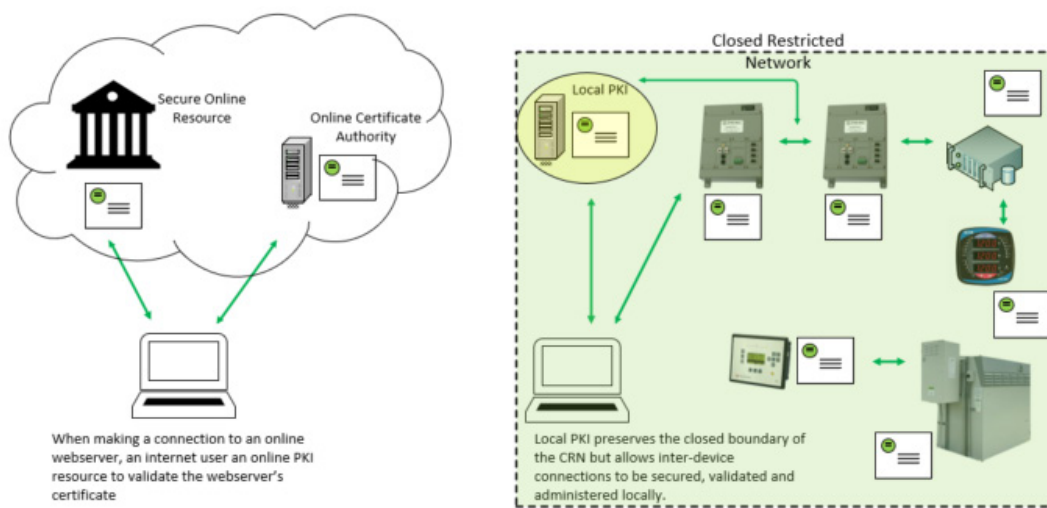


Figure 1. Using Local PKI to Secure a CRN

1.1 BACKGROUND

Common best practice for Federal control systems is to isolate the control system from other networks and from the internet. Connections to other networks are (reasonably) viewed as possible vectors for malicious intrusion, and devices on the control system network are typically not equipped with the security features which are widely available to IT devices (host-based firewalls, intrusion detection systems, anti-malware, etc.).

However, this “air gap” also isolates the system from Public Key Infrastructure (PKI) resources. Without PKI resources, the industrial network’s ability to implement strong, manageable device authentication, webserver authentication, and user authentication can be significantly reduced. Without PKI infrastructure, X.509 certificates (when used) are typically self-signed, long-lived, and difficult/impossible to manage. Revocation services are not available.

Consequently, devices on the air-gapped network operate at a diminished security posture: possibly using invalid certificates, self-signed certificates, less-secure versions of protocols, and

are non-compliant with cybersecurity requirements which would be attainable if PKI were made available. This increases the risk of unauthorized devices being connected to the network and causing harm.

This dilemma is exacerbated by the growing need to interconnect multi-vendor operational technologies (e.g., Distributed Energy Resources) within control networks to realize greater efficiency (e.g., fuel consumption reduction) and cost savings. As even air-gapped systems and networks increase in size and complexity, additional protections are necessary to secure them. Not only is device-to-device authentication needed, but also the open communication protocols that control systems commonly use must be encrypted. As the DoD moves toward “Zero Trust”, PKI-secured control systems will be crucial to supporting a framework that authenticates entities attempting to connect to its systems. PKI offers certain advantages that make it amenable for this application:

1. PKI is a mature methodology trusted worldwide to protect and authenticate our most sensitive communications across the internet (certainly an insecure medium).
2. PKI transactions are sparse and allow secure communications between devices without the need for ever-present mediation from a server, and without security applied at the network level.
3. X.509 certificate operations are supported by a variety of platforms, and not limited to a specific vendor or a platform.
4. PKI X.509 certificates as well as the protocols that use them (such as TLS) are regularly developed, evaluated, standardized, and maintained.
5. PKI implementation on a CRN can be used to not only secure inter-device connections, but also user accounts (via Client Certificates) as well as logs, files, and device configurations.

The CRN CA provides a cryptographically secure platform that is extensible, quick, and easy to deploy, cost effective and can reside on the native control system. This will reduce cyber risk with the ability to perform all PKI-based functions (e.g., certificate issuance and revocation) and operate in a resource-constrained environment.

1.2 OBJECTIVES OF THE DEMONSTRATION

The overall objective of the project was to demonstrate a low-cost solution to add the security capabilities of PKI in CRN environments that resolves the dilemma of either 1) having no access to a CA server (and no PKI capabilities) or 2) establishing interconnections that may increase the attack surface of the otherwise closed network.

The objectives of the demonstration were to explore, develop and test the application of PKI (as provided by the EJBCA platform) on a typical CRN, with representative devices, and observe and manage the system at an accelerated timeframe which includes initial enrollment, certificate expiration, revocation, and PKI interaction among the devices.

Enhanced security was an essential objective of the project. The demonstration at NREL provided an opportunity to evaluate and observe the operation of this test network, with NREL personnel recording network traffic and assuring that protocols were being executed securely and as expected during the various test scenarios. Security verifications were also performed via attempts to insert “rogue” devices onto the network and assuring that they were unable to connect. After the planned demonstration was completed, additional scenarios were examined, at the request of the NREL personnel.

To include devices and protocols which cannot support PKI, secure endpoints were developed to demonstrate a viable method of extending TLS encryption and authentication to devices which operate using serial protocols.

1.3 REGULATORY DRIVERS

The CRN CA directly addresses requirements related to PKI implementation found (but not limited to) the following directives, standards, and guidance:

- Department of Defense (DoD) Risk Management Framework and Cybersecurity directives, including related Service-specific guidance:
 - DoD Instruction 8500.01, Cybersecurity, March 14, 2014
 - DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017
- National Institute of Standards and Technology (NIST) 800 series special publications:
 - (NIST) Special Publication (SP) 800-82, Guide to Industrial Control Systems (ICS) Security, Revision 2, May 2015
 - NIST SP 800-60, Information Security, Revision 1, Volumes I & II, Information Security, August 2008
 - NIST SP 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016, Updated June 7, 2018
 - NIST SP 800-53, Revision 5, Security and Privacy controls for Information systems and Organizations, September 2020
- Whole Building Design Guide (<http://www.wbdg.org/>) publications:
 - Unified Facilities Criteria (UFC) 4-010-06, Cybersecurity of Facility-Related Control Systems, Change 1, January 18, 2017

- Unified Facilities Guidance Specification (UFGS) 25 05 11, Cybersecurity for Facility-related Control Systems, November 1, 2017
- Security Technical Implementation Guides (STIG) and Security Requirements Guides (SRG) (<https://public.cyber.mil> or <https://cyber.mil>)
- Zero-Trust Reference Guide (coming FY2021), collaboration between the Defense Information Systems Agency (DISA), National Security Agency (NSA), U.S. Cyber Command, and the private sector

2.0 TECHNOLOGY DESCRIPTION

2.1 TECHNOLOGY OVERVIEW

Demonstration of PKI on a CRN required the incorporation of several types of technology, as well as development of the selected technologies to participate in the intended use-cases.

A primary requirement was making PKI resources available to the CRN. PrimeKey's EJBCA was selected as the PKI solution. EJBCA created a local root of trust, provided device certificates to end-devices through EST, and provided validation services through OCSP and CRLs. The EJBCA also provided a secure web interface as a means of administering and monitoring PKI activities. A more detailed description of the EJBCA is provided in Section 2.1.1.

To provide a context for demonstrating PKI activities on a CRN, S&C provided a network of equipment typically found on microgrid CRNs. The provided equipment participated in the PKI services provided by the EJBCA, and various use cases were exercised to demonstrate and test the PKI implementation.

The network included several S&C GridMaster Intelligent Power Controllers (IPCs) as microgrid controllers (described further in Section 2.1.2), a Windows 10 based HMI for interfacing with the GridMaster IPCs (Section 2.1.3), a Linux based syslog server used to collect logging data (Section 2.1.4), and a Woodward LS-5 to represent a typical distributed energy resource (Section 2.1.5).

To demonstrate a method of authenticating and securing communications to the LS5, which could not support TLS connections, "Secure Endpoints" were developed and demonstrated at the NREL facility (Section 2.1.5).

To provide traffic on the network, and to exercise the GridMaster IPCs during the test, a simulation computer was added to the test network. The simulation computer provided data about the state of a simulated microgrid to the GridMaster IPCs, which allowed the performance of the controllers to be monitored and assessed during the demonstration (Section 2.1.6).

A conceptual diagram of these components (except for the simulation computer) in the context of a real-world scenario is shown in Figure 2 below.

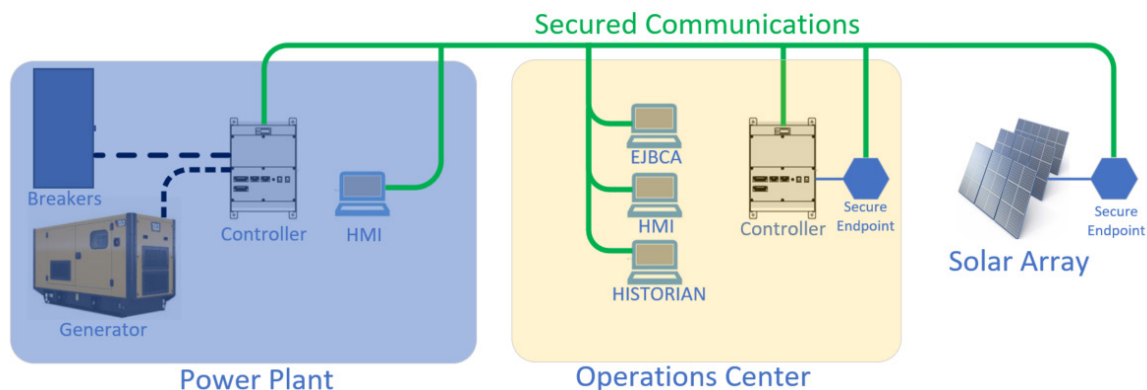


Figure 2. Conceptual Diagram of Full Solution

The following sections describe these components in further detail, as well as the development required to achieve a successful demonstration at NREL.

2.1.1 PrimeKey EJBCA

EJBCA is a standards-based PKI solution with over 15 years of continuous development and improvement. It is a Java-based Certificate Authority that can be used to issue and manage certificates. The EJBCA can store its keys software or in a Hardware Security Module (HSM) through PKCS#11 interface. EJBCA supports various algorithms as Rivest–Shamir–Adleman (RSA) or Elliptic-curve cryptography (ECC) as well as different key lengths. EJBCA uses X.509 certificates to authenticate the users accessing the administration graphical user interface (GUI). EJBCA uses role-based access control as well having support for security functions like dual authorization for administrative tasks and separation of duties. The issuance of certificates to end devices or users of the system is ultimately flexible and provided in a variety of methods including Application Programming Interfaces (APIs), protocols and web-based human interfaces. It's these APIs that allow EJBCA to connect to any variety of device that requires a digital certificate. EJBCA supports both Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) for providing revocation information to clients. The connectivity required is extremely low bandwidth and generates minimal additional network traffic. By removing the need for interconnections to an external CA server, the network can remain isolated and cyber risk to Facility-Related Control Systems (FRCS) and other control systems and critical infrastructure is significantly reduced. The PrimeKey software appliance is installed on-premises and operated from on-premises servers and virtualization resources

PrimeKey's EJBCA supports additional deployment options including a hardware appliance and software installations using EJBCA source code. The PrimeKey EJBCA Hardware Appliance deployment option is outlined in Appendix C – PrimeKey EJBCA Appliance.

2.1.1.1 EJBCA Internal Architecture

The EJBCA system architecture is comprised of:

- Operating System: A Linux based operating system
- Open Java Developer Kit (OpenJDK): is a free and open-source implementation of the Java Platform, Standard Edition. This contains the Java Virtual Machine.
- Application Server: A Java Enterprise Edition (JEE) application server providing middleware services for security, persistence, and management of resources. EJBCA supports Wildfly and JBoss Java application servers.
- Apache HTTPD: Acting as a web proxy between clients and the application server.
- Apache Ant: A build system for compiling EJBCA
- MariaDB: An SQL database supported by EJBCA
- MariaDB Java Connector: A Java application acting as a bridge between EJBCA and MariaDB

A representative software-based deployment of the EJBCA architecture is shown in Figure 3.

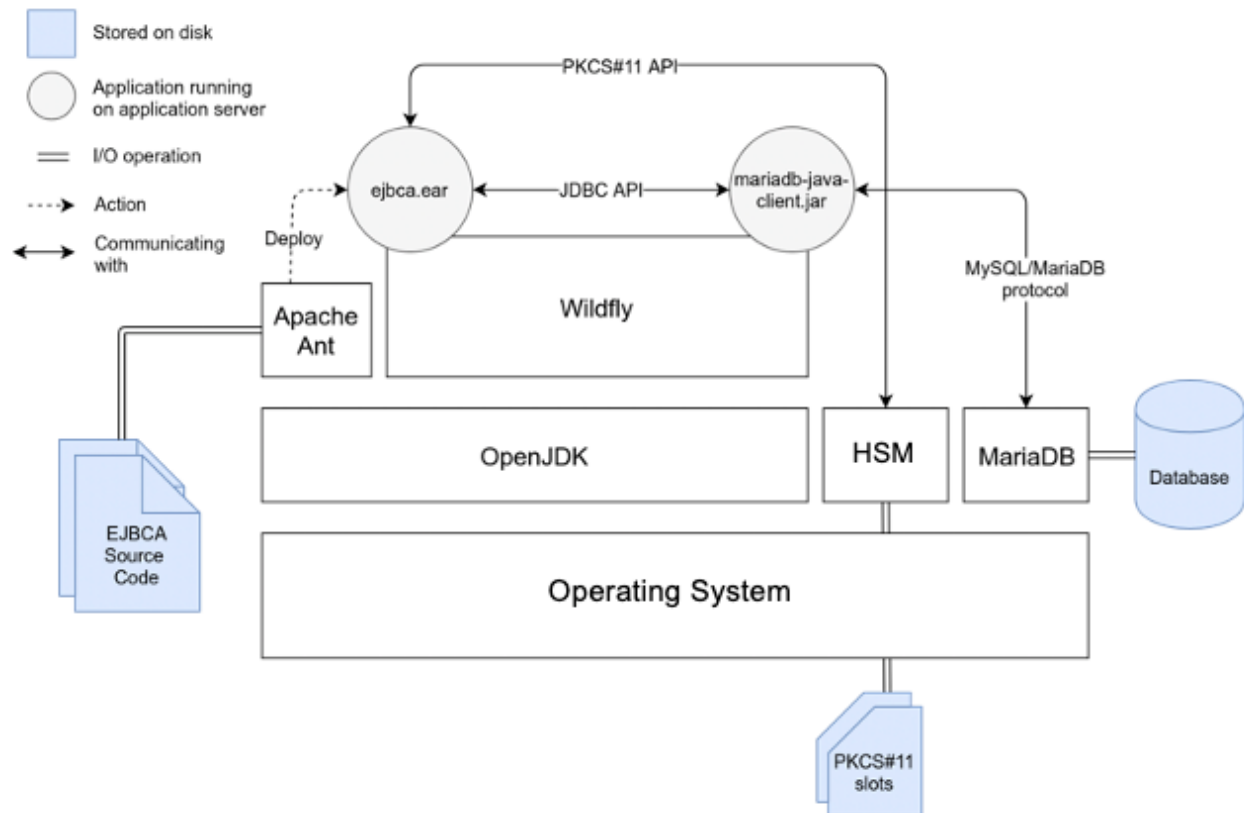


Figure 3. PrimeKey EJBCA Architecture

Internally, EJBCA utilizes web modules that are packaged as Web Archives (WAR) and packaged inside an Enterprise Archive (EAR) together with Enterprise JavaBean (EJB) modules for business logic, code for mapping Java objects to database rows and additional libraries needed by the application that are not provided by the application server. The following diagram (Figure 4) shows an outline of the internal architecture of EJBCA, and dependencies between different modules.

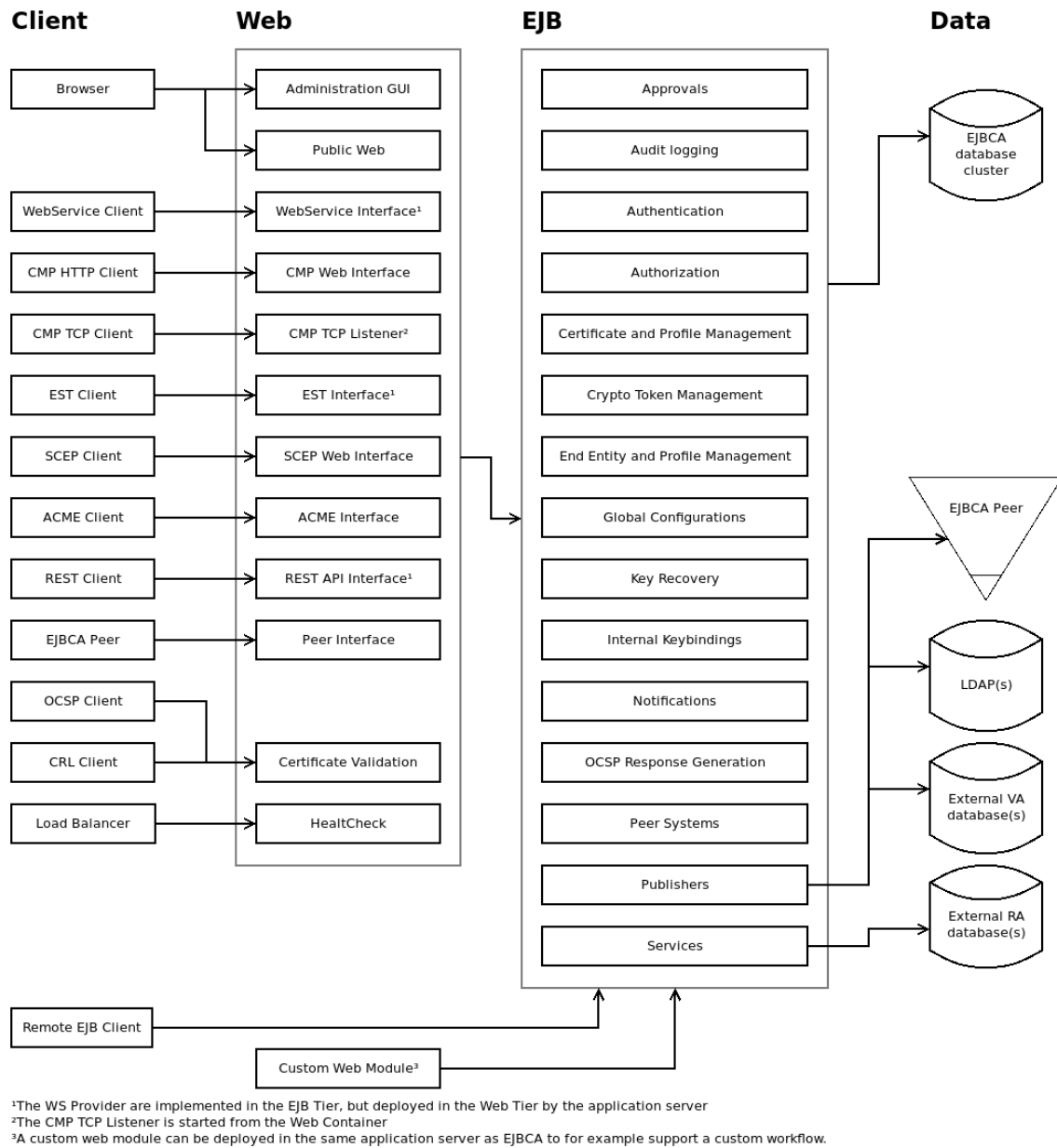


Figure 4. EJBCA Model View Controller Design

2.1.1.2 Enrollment over Secure Transport

Enrollment over Secure Transport (EST) is a certificate management protocol supported by EJBCA, which targets PKI clients that need to acquire client certificates and associated CA certificates. EST characteristics include:

- EST requests communicate over TLS
- Supports Elliptic Curve Cryptography (ECC)
- EST supports client certificate and a shared secret for authenticating with the CA
- Supports certificate renewal

Figure 5 below depicts the EST protocol between the client (GridMaster IPC) and EJBCA (CA).

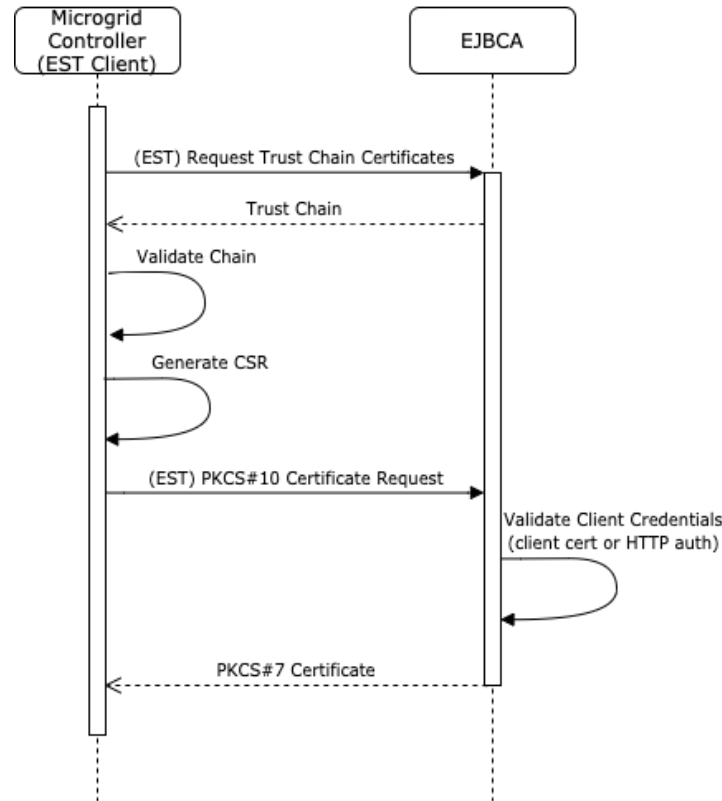


Figure 5. EST Protocol between GridMaster IPC and EJBCA

2.1.1.3 Certificate Revocation List

A Certificate Revocation List (CRL) is a list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

2.1.1.4 Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of identified certificates. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificates in question until the responder provides a response.

2.1.2 GridMaster® Intelligent Power Controller

S&C's IPERC GridMaster system (Figure 6) is a combined software and hardware platform built for advanced microgrids. The system easily integrates and communicates with a host of different distributed energy assets. It directly controls and quickly makes decisions about the assets within the microgrid, both in grid-tied and in islanded operation. It uses a distributed community of peer controllers within the microgrid network to monitor and control the various loads, power sources, and switchgear.

Typically, two or more IPCs are installed on a microgrid, for redundancy and for the distribution of connections to SCADA devices. To provide any IPC the ability to assume expanded operation of the microgrid in the event of a IPC failure, the IPCs must continuously share data, providing each controller a complete and current model of the microgrid.

To communicate with end devices and controllers, the IPC supports standard protocols, including Modbus, DNP3, Controller Area Network (CANbus), and proprietary protocols for inter-IPC communications. Communications can be made over Ethernet or over direct serial communications. The IPC is accessible to the HMI through an embedded webserver.

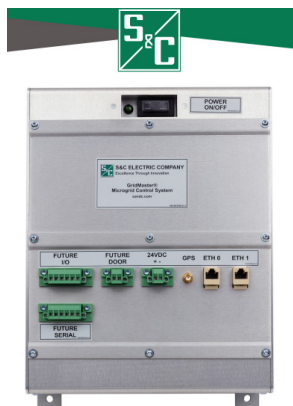


Figure 6. S&C GridMaster IPC Microgrid Controller

The GridMaster IPC was designed with security in mind and has consistently achieved compliance with DoD regulations and guidelines for cybersecurity. It has been tested and performed well under penetration tests performed by DoD personnel.

The GridMaster IPC is approximately 230 mm wide, 350 mm tall and 100mm deep. It is designed to operate in ambient temperatures ranging from -45C to 65C and easily fits inside weather-resistant enclosures. It supports two network interfaces and up to three serial connections. It contains a built-in GPS module and external antenna connection to obtain accurate time from GPS satellites. GridMaster IPCs operate on 12 to 36 VDC input and consume approximately 15 watts.

Security concerns for the IPC include making sure that communications with peer IPCs (via inter-IPC communications) with HMI computers (via the HTTPS webserver) and with end devices (such as the Woodward LS5) are encrypted and that strong device authentication is taking place before these connections are made. Using PKI to achieve these security objectives was part of the demonstration use cases.

2.1.3 HMI

HMI (Human Machine Interface) computers are used on industrial networks to provide an interface for control and monitoring of automated processes. This is a critical function on a CRN or industrial network.

A Windows 10 HMI was provisioned and included in the demonstration. The only required software for the HMI were the Windows 10 operating system and the “Edge” browser. The HMI was used to access the HTTPS interface on the GridMaster IPC, for monitoring and control of the simulated microgrid, and was also used to access the web interface offered by the EJBCA for administration of PKI.

Securing an HMI includes (1) making sure that the information that it reports is authentic and correct, and (2) ensuring that control of the system through the HMI is restricted to authorized users.

PKI was used to address both concerns. The HMI used certificates to authenticate the IPC web interface before connecting, and a client certificate installed on the HMI was used as a credential to authenticate privileged users to the EJBCA administration webpages.

2.1.4 Syslog Server

A logging server is a critical feature of industrial networks and performs the important function of collecting operational and security information from networked devices. The logs can be used to detect security events or operational failures. They are also critical in forensics, diagnosis, and for determining the impacts of a security incident.

The syslog server developed for the demonstration was a Linux-based (Ubuntu) computer which used open-source applications (Syslog-NG) to collect, organize, and archive logging data. The server represented typical “IT equipment” which would be found on an industrial network: it runs a traditional operating system, allows for custom configuration, and readily integrates with PKI.

Implementation of PKI/TLS on the syslog server insured that (1) all logs were encrypted during transport across the network, (2) rogue devices could not connect the syslog server - which could allow spurious or counterfeit logs to be created, and (3) a rogue device could not spoof the syslog server’s identity and collect logs which may be of use to a malicious actor.

2.1.5 Woodward LS5 and Secure Endpoints

The Woodward LS5 is a widely used breaker controller and encountered frequently on microgrid implementations. The LS5 is a typical of SCADA devices: it is designed for a single purpose (monitoring and controlling an electrical circuit breaker) and must act quickly and reliably. The underlying operating system is minimalist and inaccessible to the user. The LS5 uses serial protocols to interact with a SCADA controller and/or other peer devices.

Securing serial communications to the LS5 is not challenging if the controller is collocated with the device, in which case physical security can be used to protect the cabling and connection. However, if the device cannot be collocated with the controller, securing the connection can be more challenging.

Serial to Ethernet media converters can be used to transport the serial data across an Ethernet network, but most converters do not encrypt and protect the Ethernet transmissions of the serial protocols. Of the models that **do** offer encryption, none could be found which could incorporate with the local PKI infrastructure.

Secure Endpoints were developed to address this issue. As implemented at the NREL demonstration, Secure Endpoints are serial to Ethernet media converters which transport serial data securely across a TLS/Ethernet link. Secure Endpoints can incorporate with local PKI: offering the benefits of security, centralized administration, and visualization provided by local PKI.

Secure Endpoints were demonstrated as a means of securing communications to end devices which could not support TLS connections. The LS5 was used as an example, but the technology could be applied to other devices which use serial communications.

Secure Endpoints are further described in Appendix A Section A.2.

2.1.6 Simulation Computer

The Simulation Computer used for development hosted ‘GridSim’, an application developed and used internally by S&C Electric for testing microgrid sequences and algorithms. Using a custom protocol, ‘GridSim’ provides the GridMaster IPCs with data from simulated generators, breakers, meters and other microgrid devices, allowing for the IPCs to monitor a simulated microgrid as well as interact with the devices in real-time.

The incorporation of GridSim into the demonstration provided several important advantages to the demonstration and testing:

- Simulated traffic consumed network bandwidth comparable with the consumption of real devices, making the demonstration network more representative of a real-world implementation.
- The simulation provided the GridMaster IPCs with operational tasks, such as implementing algorithms and monitoring device statuses. This allowed for an assessment of the impacts of the added security features on the primary functions of the IPCs.
- Because connections to the simulated devices are *dispersed* among the IPCs (meaning that IPC 1 may handle the simulated SCADA connection to generator 1, while IPC 2 may handle the simulated connection to generator 2), inter-IPC communications were needed so that the IPCs could maintain an accurate, shared model of the microgrid. This allowed for verification of critical inter-IPC communications, which were secured as part of the demonstration.

Communications from the GridSim simulation computer were *not* secured as part of the demonstration, as the GridSim protocols would not occur in a real-world scenario.

2.2 TECHNOLOGY DEVELOPMENT

PKI services necessary for the use-cases, such as establishment of a local trusted root, CA functionality, EST, etc. were readily provided by the EJBCA appliance. Other than scripting aimed at streamlining initial deployment for CRNs, the EJBCA did not require substantial development to perform the required functions.

Development and integration efforts were primarily focused on incorporating PKI capabilities into the GridMaster IPCs and other network devices (PKI capabilities are defined in “End Device PKI Capabilities”, Section 8.1). This development was accomplished at S&C’s Denver lab with guidance and support from PrimeKey.

The following sections describe the testing environment at the Denver lab in which the required enhancements were developed, and an overview of the methodology used to prepare the devices for a successful NREL demonstration.

2.2.1 Establish Environment for Testing and Development

After the use cases were determined, an environment to perform testing and development was prepared. First steps included sourcing hardware typical of the CRNs that S&C encounters in projects. The components described in Section 2.1 Technology Overview were all installed in a testbed designated for testing the PKI implementation.

Because PrimeKey would be administering and configuring EJBCA remotely, a VPN was established to allow PrimeKey remote access to the testbed and access to the devices within it.

Test equipment was also added to the environment. To verify that unauthorized traffic was identified and dropped as expected, a network tap and Wireshark computer were connected to monitor and analyze connections on the testbed. To generate unauthorized connection attempts, a ‘rogue’ GridMaster IPC, which was not provisioned with certificates, was introduced into the testbed.

Relays and indicator lights were connected to monitor the LS5’s breaker status, to insure it was responding to commands.

Finally, a Windows 10 computer was added to the network to run VirtualBox and host the EJBCA as a virtual appliance.

2.2.2 Initial Testing and Development

2.2.2.1 EJBCA

PrimeKey deployed the EJBCA software appliance (on the hypervisor host) with a preliminary configuration tailored to the designated test cases (Section 5.4): capability of providing/renewing certificates using EST, OCSP and CRLs for certificate validation, secure key-pair algorithm for cryptographic operations, and a unique root of trust to be used for the initial tests.

The EJBCA VM (see Figure 7) was configured to use only certain ports on the host machine’s network address, and some time was spent configuring the host to make sure that only the necessary ports were forwarded to the VM from the host.

- TCP 22 – SSH access to EJBCA Software Appliance
- TCP 80 – OCSP and CRL

- TCP 443 – Administration access to EJCA AdminWeb, PublicWeb, RAWeb, and EST

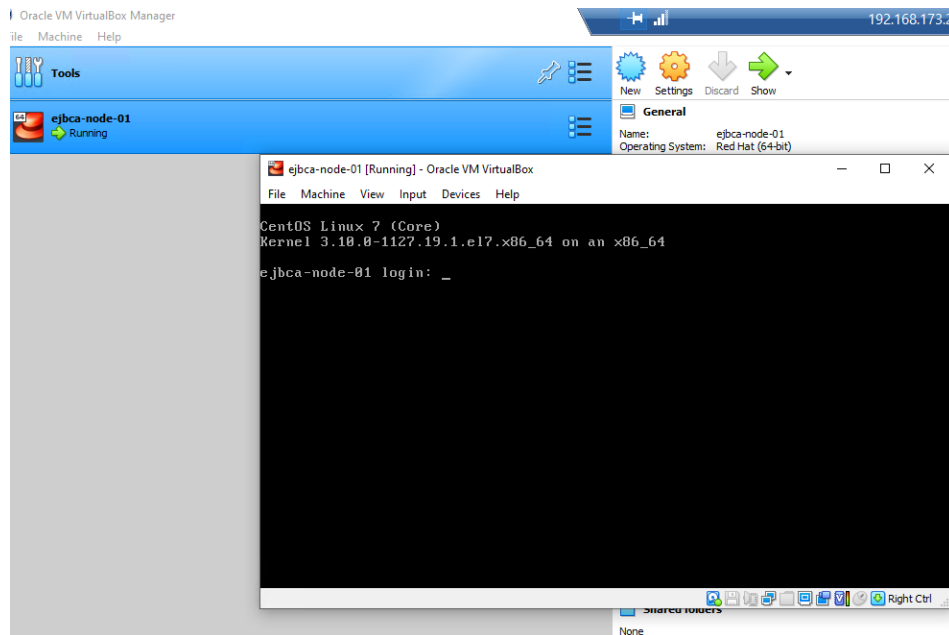


Figure 7. EJBCA running as a VM on a VirtualBox Host

2.2.2.2 EST Implementation

With the EJBCA operational, initial testing involved using the EST protocol to obtain certificates from the CA over the network. Initial testing of the EST transactions used the LibEST libraries created by Cisco; ultimately the Linux curl utility was determined to be a more flexible alternative for the specific applications that were being used. CURL was found to be well suited for dynamically generating the HTTP requests that comprise the EST protocol.

Once successful methods were established to obtain certificates from EJBCA using EST with manual command-line operations, the CURL command string was captured and inserted into a script so that the EST activity could be automated. Components of the command that would change for different devices were inserted as variables (\$1, \$2, \$3) (see Figure 8). The CURL string shown below represents a component of the scripts which were generated to automate EST transactions. The purpose and functions of the script in its entirety are more fully described in Appendix A.

```
curl -v --cacert "$1" --key $3 --cert $2 --data @$4 -o $5 -H "Content-Type: application/pkcs10" -H "Content-Transfer-Encoding: base64" https://$6/.well-known/est/$7/simplereenroll
```

Figure 8. Code Snippet Showing CURL Command with Variables

2.2.2.3 Certificate Integration

Development was done on the devices to integrate the certificates into the relevant applications, as applications are configured to access certificates and private keys in various ways. Once the certificate was obtained using EST, mechanisms needed to be identified to provision the certificate in the required keystore and restart the necessary services. The IPC's, secure endpoints, syslog server each required specific parameters for key and certificate storage. An example of the syslog-ng configuration is shown in Figure 9. Once correct storage methods were identified, scripts and utilities were developed to automate all aspects of certificate acquisition, installation, and monitoring. These scripts are described in Section 10.0.

```
destination demo_tls_destination {  
    network(  
        "192.168.8.14" port(1999)  
        transport("tls")  
        tls(  
            ca-dir("/opt/syslog-ng/etc/syslog-ng/ca.d")  
            key-file("/opt/syslog-ng/etc/syslog-ng/key.d/client.key")  
            cert-file("/opt/syslog-ng/etc/syslog-ng/cert.d/client_cert.pem")  
            crl-dir("/certstore/crls")  
        )  
    );  
};
```

Figure 9. Example of Syslog-ng Config File Showing PKI Filesystem Locations

2.2.2.4 Local User Interfaces

To allow for PKI administration of the devices without complicated command-line usage, a user interface (see Figure 10) for PKI activities was developed and installed on the GridMaster IPCs, syslog server, and other end devices which would participate in the PKI. The interface as developed and implemented is described in Appendix A. The provided interface operated over SSH and facilitated administrative activities including (1) initiating initial enrollment and allowing for the temporary credential to be provided to complete initial enrollment (2) monitoring the status of currently installed certificates on the device (3) configuring the IP address to be used for reaching the CA server (4) installing the trusted certificates from the local CA server, and (5) renewing the certificates automatically when the existing certificate's expiration date was within a predefined renewal window.

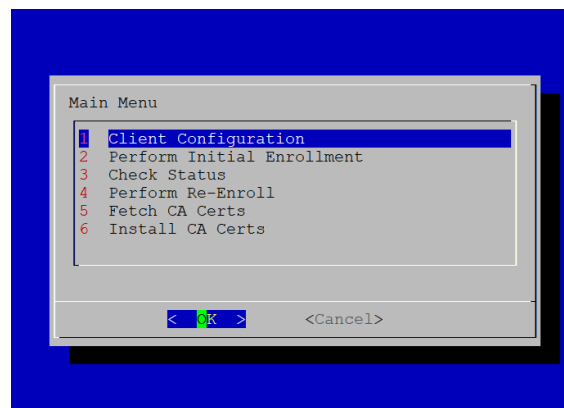


Figure 10. Local Configuration Utility on Client Devices

2.2.2.5 Initial Testing Results

As methods for participating in PKI were developed and applied, it was necessary to monitor and test the implementation. Wireshark captures were used to make sure that that traffic was encrypted as expected. Other tools such as NMAP were used to scan the listening sockets and make sure appropriate TLS protocols were being used. Latency and reliability were measured on communications across the Secure Endpoints using an oscilloscope to quantify the time delta between a signal entering the serial port of one endpoint and leaving the serial port of the other.

Long-term testing (14+ days) was done with automatic certificate renewal occurring at accelerated intervals to make sure that the certificates renewed automatically at the defined thresholds, and that the system was robust enough to overcome real-world issues such as loss of the network during PKI activities such as certificate renewal.

During testing it was observed that the Operational Technology (OT) devices tended to set up long-lasting connections, only validating the certificates during initial handshake. To enhance the security posture of the network, and to allow for revocation to have an immediate effect, regular validation checks (approximately every 30 seconds) were set up on the devices to validate certificates during active connections, rather than only at initial connection.

2.3 CRN EJBCA ADVANTAGES AND LIMITATIONS

The advantage of this solution is its widespread application in the Department of Defense (DoD) control system environments and is applicable to legacy devices as a retrofit. Other advantages and benefits include:

- Low-cost security – The level of increased security provided more than justifies the life cycle cost of the technology.
- Security where there was none – The technology enables PKI capabilities in environments where it was not possible or where not all the security properties of a certificate (i.e., self-signed certificate) that certificates signed by a CA are provided.
- Ease of deployment – simple and quick procedures to stand up the technology.
- Sub-CA capability – For already-interconnected operational networks, or if there is a case where a CRN needs to be connected to another network, the EJBCA solution may be configured as a subordinate CA to another CA.
- Zero-trust support – users and devices can be “verified” as authorized, not simply trusted if within the CRN.
- Centralized administration is possible as all certificates can be administered from the EJBCA system.
- The site can adjust the lifetimes of the certificates to appropriately balance security and ease-of-administration concerns (expiration of certificates can be adjusted to appropriate levels on a per-site basis).

- EJBCA supports the EST protocol as defined in RFC7030 as of EJBCA version 6.11. EST provides a basic protocol for certificate enrollment and management similar to SCEP, with the following distinct advantages:
 - While SCEP communicates over HTTP and ensures integrity by wrapping the payload in a cryptographic envelope, EST requests are always over TLS and thus inherently secure.
 - EST supports ECC, while SCEP does not.
 - While SCEP requires a shared secret to authenticate CSRs, in EST authentication is implicit when negotiating the TLS connection.
 - Certificate renewal is an integral part of EST, while in SCEP it is rather an afterthought.
 - EST supports server-side key generation, which SCEP does not (currently not supported in EJBCA).

The types of microgrid environment devices are distinct from those found on a typical DoD enterprise network and present challenges when implementing a PKI. These challenges are linked to the capabilities of the devices to participate in a PKI and perform cryptographic operations. These limitations include:

- Non-PKI-enabled Devices Limitation - Device in field does not support the installation of digital certificates and/or PKI libraries
 - *Mitigations:* Add a PKI-enabled device such as the “Secure Endpoints” outlined in DER/Secure Endpoints section to secure traffic to the non-PKI enabled devices.
- EST Enabled Devices Limitation – Certain Field equipment does not natively support EST
 - *Mitigations:* An EST Client like the one demonstrated can be installed on the device to perform EST operations. In addition, EJBCA offers other mechanisms (RESTAPI, ACME, CMP, etc.) for certificate management in cases where EST is unsupported by the device. Manual device certificate enrollments can be performed if no other methods are feasible.

While not a true limitation, the addition of hardware to accommodate devices that do not support PKI increases administrative overhead and potential points of failure. Risks and potential mitigations to consider include:

- CRN CA Compromised Risk – CRN CA’s private keys and/or EJBCA host is compromised.
 - *Mitigation:* Implement host-based security mechanisms to secure the EJBCA host from unauthorized access and configuration changes. Protect CRN CA keys in a hardware security module.
- Improper CRN CA Use Risk – CA performs operations that are not approved by the local PKI Policy
 - *Mitigation:* Implement a local certificate policy (CP) and certification practice statement (CPS). Perform periodic PKI audits on the CRN CA against the CP and CPS
- Private Key Compromised Risk – Unprotected private keys can be obtained and used to impersonate a trusted device.
 - *Mitigation:* Encrypt private keys and/or store in a secured file system. Additional details provided in Key Storage section

- Points of Failure Risk - Adding devices such as the “Secure Endpoints” to encrypt traffic adds potential “points of failure” to the network as well as additional requirements for administration and maintenance.
 - *Mitigations: Provision Secure Endpoints in a redundant architecture for failure scenarios (e.g., Secure Endpoint device failures), harden these Secure Endpoints, and provide clear documentation for replacement procedures.*
- Added Complexity Risk – The addition of the EJBCA CRN PKI solution requires implementing new policies and procedures that CRN administrator/operators may be unfamiliar with. For instance, when provisioning new or replacing devices on the CRN, devices will need to be enrolled in the PKI before being allowed to participate in the network with other secured devices.
 - *Mitigations: service level agreements with local network administrators, clear documentation.*

2.3.1 Alternative Technologies

Alternative PKI technologies are currently in use in CRNs. However, there are limitations and risks that need to be considered. These limitations are described below.

2.3.1.1 Self-Signed Certificates

This is the default methodology for issuing certificates in FRCS CRNs and for devices which offer webservers but do not reside on the internet. The GridMaster system offers a self-signed webserver certificate which is required to be manually imported on the HMI, and uses self-signed certificates whenever TLS is implemented. Many field devices which offer webservers also use this methodology, including Power Quality Meters, PV Cluster Managers, and other similar devices offered in a CRN.

There are many drawbacks to self-signed certificates, including:

- Self-Signed certs generally have a very long lifetime, as they are difficult to replace.
- Trusting a self-signed certificate requires installation of that certificate on every device that must trust it.
- Certificate validation of self-signed certificates is non-existent due to no authoritative source of obtaining certificate revocation information existing. To disable trust of a device’s self-signed certificate, the untrusted certificate must be removed from all devices which trusts the self-signed certificate. For example, when a device is decommissioned or replaced, the now-unused certificate must be removed from every device that trusts it.

The typical outcome is that the process of importing self-signed certificates is often neglected, and device webservers are often accessed with the browser’s “Security Warning” bypassed and ignored. This allows CRN webservers to be easily spoofed (since the warning is habitually disregarded). Additionally, some STIG settings require the browser to be configured so that it **cannot** bypass this warning, meaning that recommended security settings must be left unimplemented to allow browser access to CRN devices.

In short, extensive use of self-signed certificates creates an administrative quagmire, and a decreased security posture.

2.3.1.2 *Active Directory*

Although Active Directory (AD) *can* be integrated with PKI (as provisioned by the EJBCA), using AD requires a Windows domain implementation (which may be beyond the means and needs of a CRN) and primarily provides device security for Windows devices. Many OT CRN devices do not run a Windows operating system, and consequently would have limited access to the security features of the domain. Some distributions of Linux (e.g., RedHat) have utilities for joining an AD domain. The Linux machines could then utilize Windows' Network Device Enrollment Service (NDES) for certificate enrollments. NDES is supported by AD Certificate Services, but it uses the less secure Simple Certificate Enrollment Protocol (SCEP) and not EST.

By contrast, the functionality required to use EST and to participate in PKI is relatively lightweight and is accessible to most, if not all, platforms.

2.3.1.3 *Network Level Security*

The most often-used network security measures are focused on the perimeter of the network (e.g., firewalls or routers). This technology is not helpful in securing inter-device connections on a CRN and typically does not support security of FRCS protocols.

Other network security controls operate within the network, such as MAC-level or IP-level security at switchports. These techniques, however, can create a rigid network which prohibits actions like moving a device from one switchport to another, or replacing a device. Moreover, MAC and IP addresses are easily spoofed, whereas an X.509 device certificate is very difficult, if not impossible, to spoof. MAC or IP addresses are not considered strong device authenticators, and this is all that is accessible as a credential on the network layer.

802.1X is another network security control which requires authentication to a server before access to the network is granted through a switchport. This authentication requires client-side functionality which may be difficult to implement on OT devices; some devices will likely need to fall back to MAC authentication which is considerably less secure.

Additionally, network security does not solve issues with browser security warnings, as TLS will still operate using certificates without PKI services and without a shared root of trust for the CRN. Browser warnings will still appear, and likely be bypassed. Network security cannot be integrated and co-administered with other security controls, such as user accounts, whereas PKI can integrate a whole site into a single root of trust and be used to regulate human activity as well as inter-device activity.

3.0 PERFORMANCE OBJECTIVES

Performance objectives are targets for assessing the technology. They provide a framework for evaluating the performance goals of the project. The following Table 2 summarizes the performance objectives established for this project, and whether those objectives were met.

Table 2. Performance Objectives

Performance Objective	Metric	Data Requirements	Success Criteria	Results
Quantitative Performance Objectives				
Quick EJBCA Deployment	Duration of EJBCA deployment activities	Representative control system administrator start-to-finish time for deployment activities	<60 minutes	Pass
Low Level of Effort for Realized Capabilities	Score of Ratio of adjustments to new capabilities	List of adjustments needed to stand up EJBCA with weighted levels of effort, list of additional capabilities with weighted values	Overall score indicates value of capabilities realized (benefit) outweighs the level of effort to implement (cost)	Pass
Enhanced Security	Additional cybersecurity requirement compliance enabled.	Baseline of PKI security requirements that are non-compliant without PKI capabilities	>90% compliance of PKI security control requirements dependent on access to a CA server (See Appendix D – PKI Authentication STIG Requirements)	Pass
Qualitative Performance Objectives				
Ease of Use	Interviews of DoD components on ease of implementation	Interview results	Average responses indicate positive attitude or opinions on ease of use of the solution	Pass
Enhanced Security	Interviews of DoD components on enhanced security	Interview results	Average responses indicate positive attitude or opinions on enhanced security from deploying the solution	Pass

3.1 PERFORMANCE OBJECTIVES DESCRIPTIONS

The following sections provide further information regarding the quantitative and qualitative performance objectives as stated above.

3.1.1 Quantitative Performance Objectives Descriptions

3.1.1.1 Quick EJBCA Deployment

- Purpose: To demonstrate the ease of use in standing up PKI capabilities in a CRN typically seen in DoD control system environments.

- Metric: The overall score of a level of effort for the adjustments required to stand up a working EJBCA solution in a control system environment vs. the weighted value of the security capabilities added or enabled by EJBCA.
- Data: Timed deployment of EJBCA.
- Analytical Methodology: A user unfamiliar with EJBCA will represent a control system administrator to deploy EJBCA in the test VM environment.
- Success Criteria: EJBCA is deployable in under 60 minutes.
- Results: EJBCA was deployed on the test bed in 30:29 minutes.

3.1.1.2 Low Level of Effort for Realized Capabilities

- Purpose: To validate the cost/benefit of enabling PKI in DoD control system CRN environments.
- Metric: The number of additional cybersecurity requirements can be compliant (i.e., “Not A Finding”) when the CRN EJBCA is implemented. This are pulled from STIGs and security control correlation identifiers (CCIs) in the RMF process.
- Data: A list of adjustments needed to stand up EJBCA with weighted levels of effort, and a list of additional capabilities with weighted values.
- Analytical Methodology: Levels of effort will be weighted according to degree of difficulty/experience required, required duration, incremental cost (\$). The value of the additional capabilities will also be weighted according to potential scalability, applicability to DoD DER protections, and added security controls compliance.
- Success Criteria: The overall score indicates the value of implementing the CRN EJBCA outweighs the level of effort to implement.
- Results: The level of realized capability of the enhanced security of EJBCA PKI in the CRN exceeded the level of effort to deploy the solution.

3.1.1.3 Enhanced Security

- Purpose: To demonstrate the enhanced security from enabling PKI in DoD control system CRN environments.
- Metric: The number of additional cybersecurity requirements can be compliant i.e., “Not A Finding”) when the CRN EJBCA is implemented. These are pulled from STIGs and security control correlation identifiers (CCIs) in the RMF process.
- Data: A baseline list of PKI-related requirements for which control system owners must typically have waived due to lack of ability to comply.
- Analytical Methodology: The baseline list will be reviewed, and a determination made if EJBCA enables compliance for each requirement.
- Success Criteria: To achieve a greater than 90% compliance of the baseline list of typically non-compliant PKI security control requirements is required for success listed in Appendix D – PKI Authentication STIG Requirements.

- Results: The integration of EJBCA with the GridMaster system provided enhanced security to the FRCS CRN and greater than 90% compliance of the baseline list was met.

3.1.2 Qualitative Performance Objectives Descriptions

3.1.2.1 *Ease of Use*

- Purpose: To validate the ease of use in standing up PKI capabilities in a CRN typically seen in DoD control system environments.
- Metric: Level of positive attitudes/opinions of DoD components regarding ease and speed of EJBCA deployment.
- Data: Interview results.
- Analytical Methodology: A set of questions will be posed to DoD component representatives after presenting the CRN EJBCA concept, deployment process and results of control system admin-representative deployment test results. Discussions outside of the questions will also be captured and included in the analysis.
- Success Criteria: If the average responses indicate a positive view of the ease of deployment/use, this indicates success.
- Results: Positive feedback was received regarding the ease of deployment/use of this solution.

3.1.2.2 *Enhanced Security*

- Purpose: To validate the enhanced security enabled by standing up PKI capabilities in a CRN typically seen in DoD control system environments.
- Metric: Level of positive attitudes/opinions of DoD components regarding enhanced security.
- Data: Interview results.
- Analytical Methodology: A set of questions will be posed to DoD component representatives after presenting the CRN EJBCA concept and the security enhancements (e.g., added compliance, increase of encryption footprint). Discussions outside of the questions will also be captured and included in the analysis.
- Success Criteria: If the average responses indicate a positive view of enhanced security, this indicates success.
- Results: Positive feedback was received regarding the level of enhanced security provided by EJBCA in a CRN.

4.0 FACILITY/SITE DESCRIPTION

The demonstration was conducted at NREL's Energy Systems Integration Facility (ESIF) in Golden, Colorado in one of the lab bays. Monitors were provided by NREL staff for the demonstration along with other peripheral devices. The ESIF has many energy research-enabling capabilities and provided an ideal environment for the demonstration.

5.0 TEST DESIGN & DEMONSTRATION

The following sections describe the PKI implementation that PrimeKey and S&C Electric demonstrated at NREL in June 2021. The goal of the demonstration was to examine a representative network that incorporated local PKI on a CRN, and to evaluate the benefits and feasibility of applying this technology.

5.1 CONCEPTUAL TEST DESIGN

To thoroughly examine the PKI implementation, the demonstration required an operating network of devices and communications typical of a real-world CRN. The CRN CA was deployed in an offline, air-gapped environment and used CA signing to maintain a trust chain without needing external connectivity. PrimeKey’s EJBCA was used to provide all PKI services to this network. The EJBCA is described in detail in Section 2.1.1.

Participating network devices used a variety of platforms and included S&C’s GridMaster microgrid controllers, a Windows HMI, a Linux Syslog server, a Woodward LS5, and S&C’s “Secure Endpoints”. These devices and the development performed on them for the demonstration are described in Section 2.0, “Technology Description.”. A primary objective of the demonstration was to authenticate and secure the communications among all the networked devices, using local PKI as the trust anchor for the entire network.

In addition to the operation of PKI on the network and the security benefits achieved, the NREL demonstration was designed to show the deployment and implementation of PKI. This was done to address real-world concerns about the required level of effort and necessary PKI expertise to deploy the technology. For that reason, the demonstration started with the representative devices running without PKI enabled and the first test cases involved setting up the PKI services. On the EJBCA server all site-specific configurations were applied as part of the demonstration, and the CRN’s local “root of trust” was established. Test-case #1 details how initial EJBCA configuration was tested and demonstrated at NREL. Once PKI resources were established, all other network devices were enrolled with the local PKI as part of the demonstration. These actions were facilitated by a user interface and helper scripts that were designed to facilitate PKI operations, including initial enrollment. Initial enrollment of end devices comprises Test Case #2.

To address the administration of the network over time, other demonstrated test-cases examined revocation of certificates, renewal of certificates (manually and automatically), certificate expiration, and decommissioning of equipment. These Test Cases are described in more detail in Section 5.4.

Because industrial devices perform critical and time-sensitive operations, it was necessary to verify that the devices continued to perform required functionality concurrent with the application of the added PKI security controls. To observe and monitor the GridMaster IPC’s functionality, a simulated microgrid was incorporated into the testbed and demonstration. This interacted with the GridMasters during the test and allowed the functionality of the GridMaster IPCs to be monitored as the various use cases were implemented. The simulation computer is described in Section 2.1.6.

To demonstrate the effectiveness of the PKI implementation in maintaining a secure network, rogue devices were inserted into the network to verify that these devices were unable to connect to the PKI-enabled devices. This testing is described in Section 5.4, Test Case #6. Additionally, Wireshark packet captures were done to monitor the activity on the network to verify that valid device connections were successfully made, while invalid connections were rejected.

To allow for extension of encrypted communications out to CRN endpoints, such as the Woodward LS-5, Enrollment over Secure Transport (EST)-capable devices, referred to as “secure endpoints,” were collocated with the LS5. The endpoints perform encryption and decryption for DERs not capable of participating in PKI. The “Secure Endpoints” are media converters which convert serial data to secure TLS ethernet packets for transport over an insecure network. Secure Endpoints are described in Section 2.1.5 and were tested in Test Case #7.

Since PKI implementation does not rely on network configuration for security (PKI was designed to operate over insecure networks), the network was basic and consisted of a single subnet. As is typical in CRNs oriented towards industrial use, there were no DHCP services or DNS provided. Device access was through IPV4 address. Inter-device network connections were provided by a Cisco IE4000 managed switch.

5.1.1 Demonstration Test Phases

This section describes the demonstration test phases, from setup to installation/implementation to demonstrating and evaluating the solution.



Figure 11. Demonstration at NREL

5.1.1.1 NREL Testing Environment Hardware Setup

1. All required hardware was supplied and brought to NREL by S&C/PrimeKey, including power supplies and equipment to be demonstrated. Power supplies operated on standard 120V single phase power and did not require substantial power (<500W) to operate.
2. A vertical plane was used to mount the GridMaster controllers and other wall-mounted equipment, for ease of viewing during the demonstration.
3. Several pieces of IT equipment (syslog server, HMI, and EJBCA) were connected to the network and located on a table near the vertical plane.
4. To provide an accurate time-source to the network, one of the three GridMaster IPCs connected to an NREL-provided antenna for access the GPS network. All PKI participating devices, including the EJBCA, were configured to synchronize with this GridMaster system's clock. Accurate time is important for successful PKI operations.

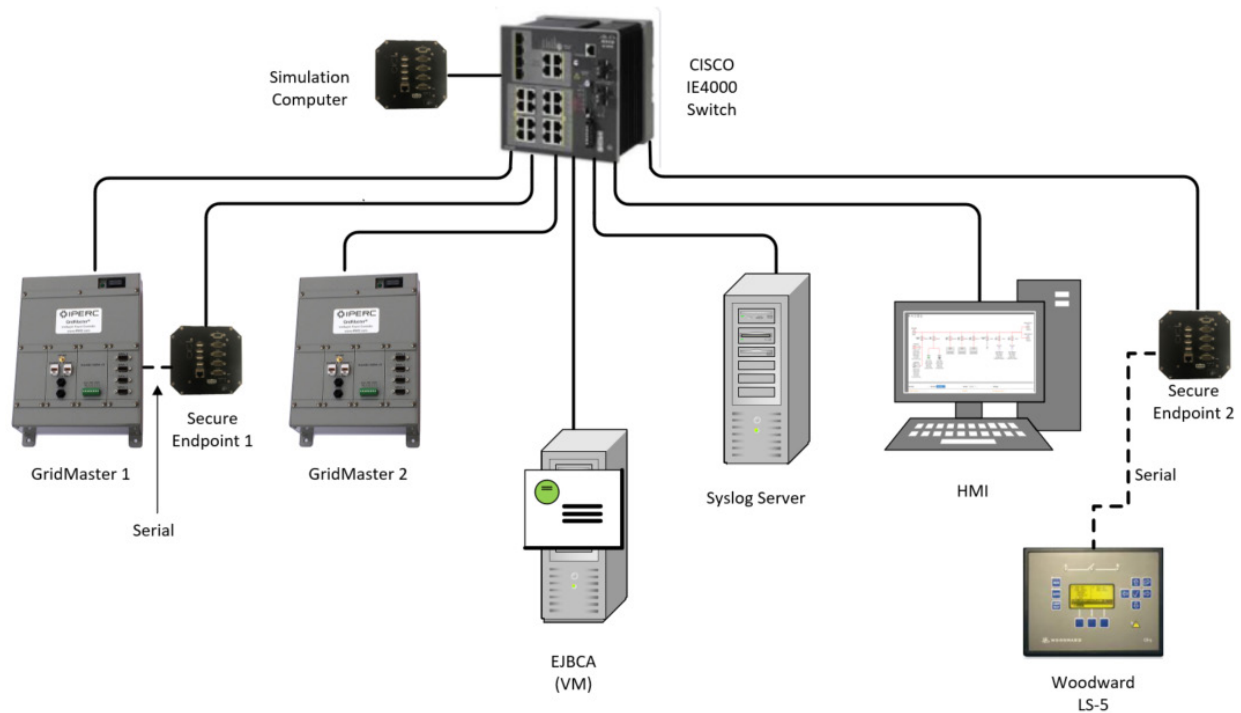


Figure 12. Testbed Setup

5.1.1.2 Baseline Characterization Phase

The simulation computer was started, and multiple baseline packet captures were made by NREL personnel of the inter-device unencrypted traffic. This constituted the “Baseline Characterization” described in Section 5.2.

5.1.1.3 Testing Phase (Exercise of the Test Cases)

This phase encompassed the bulk of the demonstration. Since initial deployment was part of the testing, initial deployment **and** all subsequent testing performed in this phase are defined in the Test Cases (Section 5.4).

The EJBCA server was installed and initialized as a Virtual Machine. PrimeKey performed installation and site-specific setup on the EJBCA, analogous to what an onsite administrator would perform to initially commission the equipment.

First-time certificate enrollment was performed on the GridMaster IPCs and other secured end-devices using the developed custom scripts and UI. It is anticipated that a UI to facilitate PKI operations would become part of the standard deployment for S&C products that use PKI.

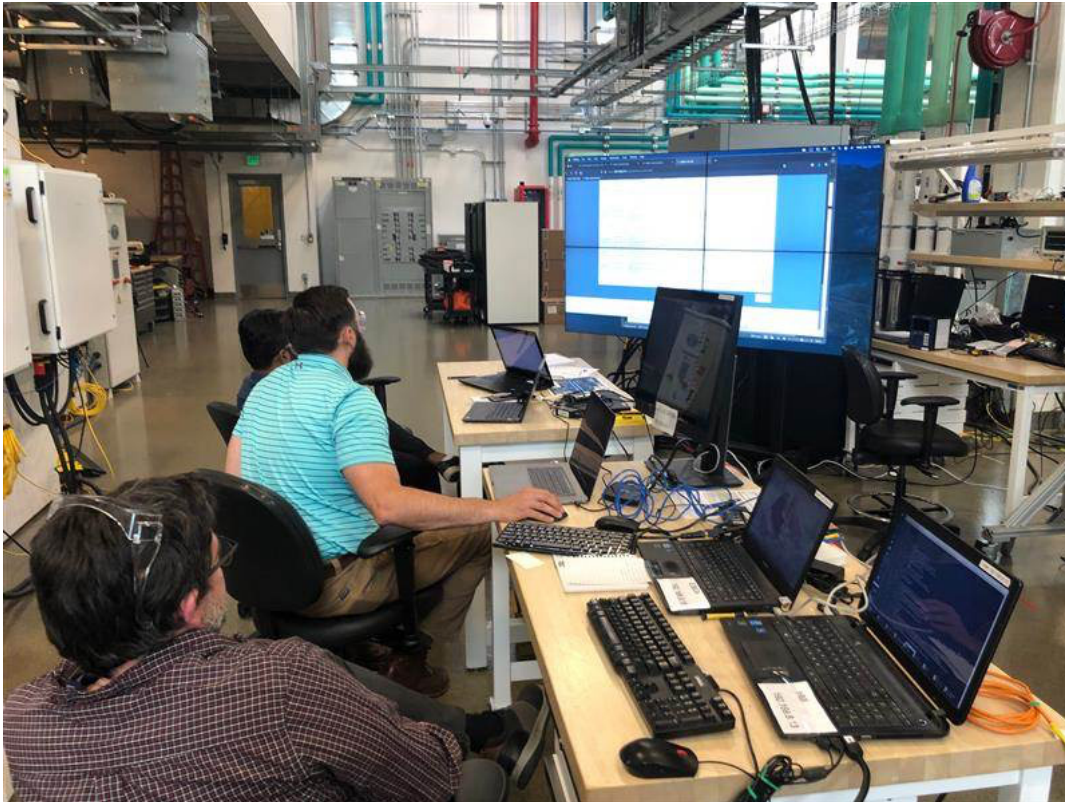


Figure 13. Demonstration at NREL

The various tests were performed which include demonstration of automated certificate renewal, certificate revocation, and attempted penetration of the network by unauthorized devices.

5.1.1.4 Testing Performed at Request of NREL

After the prepared test cases were completed, some additional testing was performed at the request of NREL personnel. This revolved around the protection of certificates that had been replaced but had not yet expired. This is described in Section 6.0.



Figure 14. Demonstration at NREL

5.2 BASELINE CHARACTERIZATION

To establish a baseline, all participating CRN devices used unencrypted inter-device network communications. Logs were sent unencrypted to the syslog server, synchronization communications between the GridMaster IPCs were sent unencrypted, and Modbus data sent to the LS5 was unencrypted. Devices “authenticated” to each other only via IP address. Because the IPC webserver only operates as an HTTPS server, the webserver traffic could not be unencrypted. However, the webserver was configured to use a self-signed certificate, which caused the HMI browser to show a certificate warning.

This allowed NREL personnel to obtain packet captures of the unencrypted traffic, for use as comparisons to the traffic after encryption was applied. Additionally, due to the operation of the simulated microgrid during the test, the behavior of the system was able to be assessed starting at this point and could be monitored continuously throughout the remainder of the demonstration. This indicated that inter-device communications were active, and the system was operating successfully, although in an insecure state.

5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS

The following sections provide a more detailed description of how the tested components were operating and configured during the NREL demonstration.

CRN PKI Demonstration Network

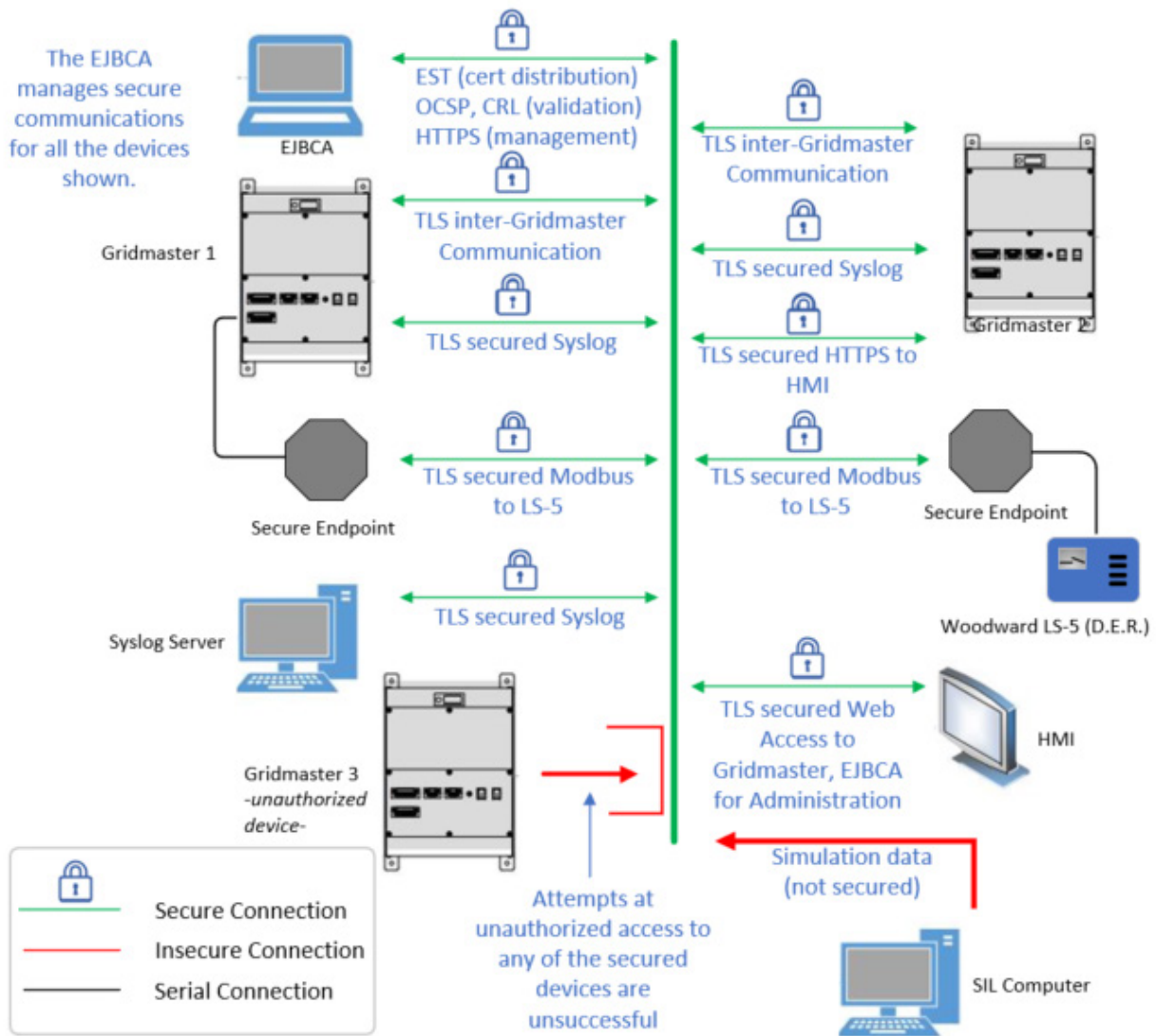


Figure 15. Conceptual Setup and Connectivity of the CRN EJBCA CHIL

5.3.1 EJBCA Integration

The EST integration points were configured on the PrimeKey EJBCA CA node to support certificate enrollment and reenrollment. In addition, EJBCA provided validation services via CRLs and OCSP.

5.3.1.1 EST

EJBCA's EST service was configured with multiple EST aliases for GridMaster devices and other types of devices. The aliases supported the different CRN devices and the type of certificate required. Both aliases allowed CRN devices to perform initial enrollments (simple enroll requests) using HTTP auth (shared secret). Re-enrollments required client authentication using the CRN device's valid CRN CA issued certificate.

5.3.1.2 OSCP

OCSP revocation services were provided by the EJBCA Node. The revocation services are available to the internal network. OSCP Uniform Resource Locators (URL) and Authority Information Access (AIA) were included in the Issuing CA certificates and end entity certificates.

5.3.1.3 CRLs

CRLs for the CA cluster were hosted on the EJBCA Node and available for download. CRL Distribution Points (CDP) were included in the Issuing CA certificates and end entity certificates.

5.3.2 GridMaster® Microgrid Control System

5.3.2.1 GridMaster Intelligent Power Controller (IPC)

The PKI-provisioned IPCs (IPC 1 and 2) communicated with each other over encrypted channels (using PKI-provisioned certificates) to synchronize their internal model of the status of the microgrid and to respond to the needs of the microgrid based upon their interpretation of the state of the grid. Inter-IPC communication is essential to allow for fault tolerance, synchronization of the shared model of the status of the grid, and to allow IPCs to keep loads and sources within pre-defined parameters.

Additionally, the IPCs reported security-related events in real time to the syslog server, and one IPC provided a webpage viewable on the HMI showing the status and allowed for interaction with the simulation. One IPC communicated with the LS-5 over encrypted serial communications (encrypted via the Secure Endpoints).

5.3.2.2 Grid Simulation (GridSim)

The simulated microgrid ran throughout the demonstration and provided interactive data for the IPCs. This provided realistic data flows on the network and allowed the operation of the HMI and GridMaster IPCs to be monitored.

5.3.2.3 Human Machine Interface

The GridMaster system visualization occurred on the HMI's browser, as shown in Figure 16, through an HTTPS webserver provided by one of the GridMaster IPCs. Communications was secured via TLS using a certificate provisioned by the EJBCA.

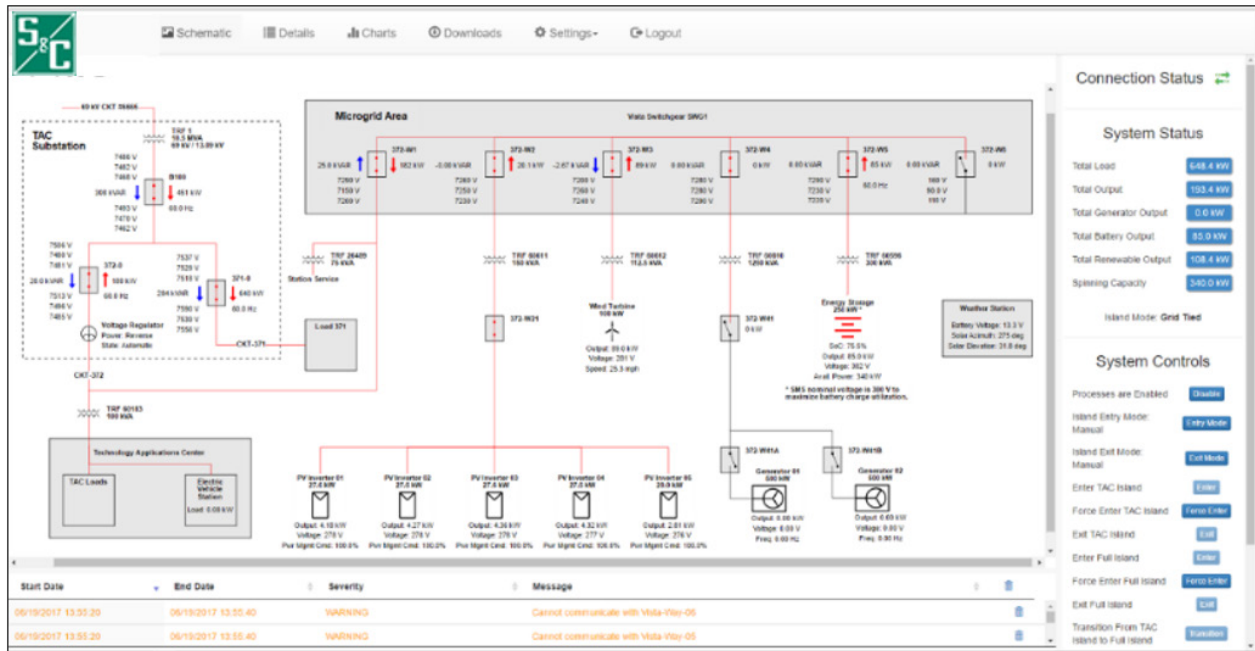


Figure 16. Typical GridMaster System HMI Graphical User Interface

5.3.3 DER/Secure Endpoints

During the test, one of the IPCs communicated with the LS-5 securely through a TLS encrypted tunnel provided by EST-capable Secure Endpoints. The certificates used in this connection were issued by the EJBCA system and the endpoint devices were managed through the EJBCA (certificate revocation, renewal, etc.) in the same manner as the other devices which participated in the secured network. Wireshark captures of these secured serial/Ethernet communications showed that these communications successfully implemented TLS, allowing for assurances of their confidentiality, integrity, and authenticity.

5.3.4 Syslog Server

A syslog server was provided to collect log data generated by various components on the CHIL network. The GridMaster IPCs and Secure Endpoints sent logging information to the server in “real time.” The syslog server provided a GUI which allowed the operator to manually inspect, and query logged data. It also offered a selection of predefined queries to detect security events which could warrant further investigation. Queries were configured specifically for this demonstration which identify PKI-related activities as they occurred in real-time. Communications to the syslog were secured via TLS with certificates issued by EJBCA.

5.3.5 CHIL Network

During the demonstration, the network used typical bandwidth as seen in a real-world CRN: communications to the SIL computer supplied realistic traffic, and any errors in communication were visible via the HMI computer and syslog server.

Communications paths typical of a microgrid network were secured as shown in Figure 15, and as described in the test cases, the security of these communications was demonstrated in real time.

5.4 OPERATIONAL TESTING

To evaluate the performance of the proposed PKI implementation, seven test cases were developed and implemented in sequence during the NREL demonstration. This was the primary testing performed for the demonstration and was oriented towards assessing the operation of PKI on a CRN, over a wide time frame, and in a variety of anticipated scenarios.

Each test case identified pre-conditions that must be satisfied before performing the test, the expected outcome for the performed test, and the test case steps. A test case PASSED if the following conditions are met:

1. The pre-conditions of the test case are fulfilled
2. The steps lead to the expected outcome

If more than two test cases failed in sequence, the entire item would be suspended following system rectification. Testing would then be resumed from the beginning (i.e., 1.X).

To validate the CRN-specific PKI functions, the following use cases were demonstrated:

- Test Case #1: Quick Setup and Configuration of EJBCA

Initial State: Windows 10 laptop with hypervisor.

Outcome: EJBCA running on the hypervisor, configured with the necessary parameters to function as a root of trust on the testbed CRN.

Metric: <60 minutes setup

- Test Case #2: End Device Certificate Enrollment

Initial State: GridMaster IPCs and other end devices use self-signed certificates (for Webserver) or communicate in plain text (all other protocols).

Outcome: Each end device is enrolled with unique server authentication certificate(s) from trust anchor.

Metric: Demonstrable (i.e., padlock icon displayed on HMI web browser and GridMaster system GUI status links show links are up) secure peer-to-peer communications utilizing cert chain from Use Case #1.

- Test Case #3: Automatic Renewal of Certificates

Initial State: The IPC's server authentication certificate issued by the trust anchor is within the certificate renewal window.

Outcome: The IPC's certificates are automatically renewed prior to expiration.

Metric: Updated certificate details show renewal; connections are reestablished with newly issued certificate.

- Test Case #4: Renewal of Expired Certificates

Initial State: IPC's server authentication certificate is expired.

Outcome: With simple administrative action, certificates are renewed, despite device being turned on/reconnected with expired certificate.

Metric: Updated certificate details show renewal, connections are reestablished with newly issued certificate.

- Test Case #5: Certificate Revocation

Initial State: IPC has a valid server authentication certificate issued by the trust anchor.

Outcome: Microgrid controller's server authentication certificate is revoked.

Metric: Web server connection is not secure, OCSP status check request shows revoked.

- Test Case #6: Unauthorized Devices

Initial State: IPC does not have a valid server authentication certificate issued by the trust anchor.

Outcome: Microgrid controller is unable to establish a connection through SSH or through inter-IPC communications. Although the IPC will host a website, it is shown as insecure when accessed by the browser of the HMI.

Metric: Access to other microgrid devices over secured protocols fails.

- Test Case #7: Distributed Energy Resource (DER) Protection

Initial State: Wholly unencrypted (Modbus/TCP) communications between the IPC and Woodward LS-5 synchronizer controller

Outcome: Wireshark packet capture shows that Modbus communications are between secure endpoints collocated with the IPC and DER.

Metric: Wireshark capture showed that the endpoints were verified using TLS certificate-based encryption and ethernet traffic could not be manipulated.

6.0 PERFORMANCE ASSESSMENT

Demonstration of the technology as described above was performed at NREL in Colorado in June 2021. The qualitative and quantitative objectives were met. See Table 2 – Performance Objectives.

The demonstration began with a complete baseline configuration on all participating devices, including the EJBCA. PKI services were installed and configured on the EJBCA, configuring a root of trust specific to the site and demonstration, and the EJBCA was configured with appropriate settings to support the intended use cases. The CRN devices (GridMaster IPCs, Syslog Server, etc.) were also configured (as part of the demonstration) to participate in the local PKI provided by the EJBCA. This was done to show the level of effort involved for initial configuration.

Once devices were configured and enrolled, automatic renewal of certificates was demonstrated, as well as certificate revocation and other security facets of PKI which were now accessible to all the devices.

Wireshark captures of various dataflows were analyzed to verify that inter-device communications were adhering to the expected, secure protocols. These captures were compared with baseline captures of the same transmissions to verify that encryption and authentication were occurring.

Testing and demonstration included attempts to insert rogue devices into the network; logs and packet captures were reviewed to assure that these rogue devices could not connect.

At the end of the demonstration, scenarios were added to assess cybersecurity aspects which were of interest to NREL personnel. Specifically, restrictions were added which helped to protect keypairs on decommissioned equipment by revoking a certificate as soon as it had been used as a credential to receive a new certificate. This feature was determined to be a valuable security asset, easily configurable on the EJBCA, and likely to be incorporated in real-world use of this technology.

Ultimately, the demonstration proved the utility of adding local PKI to a closed network as a means of securing communications between a diverse group of equipment. It showed that the PKI as implemented by the EJBCA provided for centralized security administration, accessible to operators and administrators without extensive PKI knowledge and familiarity.

7.0 COST ASSESSMENT

The cost of setting up a PKI implementation in a FRCS CRN (which is assumed to be a relatively small network) will be primarily driven by different factors. These different factors include costs associated with establishing PKI resources for the site, costs associated with implementing PKI capability on end devices on the CRN, as well as level of PKI expertise within FRCS.

7.1 COSTS ASSOCIATED WITH ESTABLISHING PKI RESOURCES FOR THE CRN

The EJBCA, which implemented all PKI resources for the NREL demonstration, does not require expensive hardware and can run on typical server or workstation platforms. For industrial environments, it can be delivered with a hardened hardware platform.

The PrimeKey EJBCA software appliance cost is approximately \$27K. Additional costs for configuration, and support are estimated separately.

Therefore, the cost of the EJBCA and its setup can be easily determined and will not be driven extensively by site-specific considerations.

7.2 COSTS ASSOCIATED WITH IMPLEMENTING PKI CAPABILITY ON END DEVICES ON THE CRN

PKI methods are accessible to a wide variety of operating systems and platforms: software libraries for EST (which was used for obtaining certificates from the EJBCA), and OpenSSL (which was used for client-side certificate operations such as validation and key/CSR generation) are open source and free.

However, as with many open-source libraries and methods, effort and cost will be consumed in implementation of PKI capabilities on the devices themselves. These are not out-of-the box solutions and must be tailored to each specific device using them. The level of effort will be determined by several factors:

7.2.1 Device Type

- 1) For **IT devices**, such as the *Windows* HMI and *Ubuntu* Syslog Server used in the NREL demonstration, the OS is accessible to the customer and already possesses the necessary capabilities for validating certificates and can readily incorporate EST for obtaining them (with a moderate degree of scripting, described in more detail within the report). Although not completely trivial, the methods are well established and available.
- 2) For Operational Technology (OT) devices which run an operating system inaccessible to the user, support from the OEM would be required to configure the required capabilities. This cost and level of effort would vary depending on the level of automation desired, the degree to which the device already supports PKI functions, and the willingness of the OEM.
- 3) OT devices which do not run an operating system (run real-time executables) present the greatest challenge. The LS5 used at the demonstration is representative of this type of device.

For the NREL demonstration, “Secure Endpoints” which participated in PKI were developed and demonstrated to work around the device’s limitations. Presently this solution is not commercially available. Attempts to locate serial to Ethernet converters that encrypted connections and used PKI were unsuccessful but may be developed in the future.

7.2.2 Device Type Uniformity

Clearly, it is more cost effective to develop implementation methods for a device-type once and apply those methods multiple times. If a network consists of many of the same or similar devices, implementation can be streamlined. Additionally, in the case of OT devices where OEM participation is required, a customer who possesses multiple ‘widgets’ from an OEM has more leverage in requesting custom functionality.

7.2.3 Level of Automation

The degree to which participation in PKI is required to automated will also drive the cost and effort involved in integrating PKI with a device. Site requirements will determine if features such as automated renewal, or ease-of-administration are necessary. CRNs oriented towards industrial use often require high-availability and are not staffed with traditional IT administrators, so it is likely that streamlining, simplifying, and automating PKI administration **will** be necessary.

7.2.4 Level of PKI Expertise

Another cost driver is the level of expertise of FRCS cybersecurity personnel. If outside support for engineering the environment for PKI and standing up the EJBICA is required, costs will be relatively higher and will vary based on the number of end devices in the environment, for example.

7.3 COST MODEL

The following Table 3 shows a sample cost model for implementing a CRN PKI Certificate Authority for Facility-related Control Systems.

Table 3. Cost Model for a CRN PKI CA for Facility-related Control Systems

Cost Element	Data Tracked During the Demonstration	Estimated Costs
EJBCA PKI Software Appliance	Estimates made based on component costs for demonstration	\$27K
Client Configuration Changes	Estimates made based on labor hours and rates for configurations required for the demonstration	GridMaster IPC: \$20K Secure Endpoint: \$8K
Secure Endpoint	Estimates made based on component costs for demonstration.	\$1K (Indoor) \$2K (Outdoor)
Installation Costs	Labor required to install and configure the EJBCA	\$30K+
Maintenance	• Frequency of required maintenance • Labor and material per maintenance action	EJBCA: \$11.5K annually
Hardware Lifetime	Estimate based on representative components depreciation	Secure Endpoint: \$0.3K annually
Operator Training	Estimate of training costs	EJBCA: \$2K

The following sections provide further information regarding each cost element.

7.3.1 EJBCA PKI Software Appliance

- Description of Cost Element: The PrimeKey EJBCA PKI Software Appliance is a required component and provides the Certificate Authority for the CRN PKI.
- Supporting Cost Data: Current commercial pricing for the EJBCA Software Appliance.
- Scalability: The cost for the EJBCA PKI Software Appliance can easily be scaled, depending on the number of appliances needed for each customer's environment.

7.3.2 GridMaster IPC – Representative FRCS

- Description of Cost Element: The GridMaster IPC is the representative FRCS device that would run the EST client.
- Supporting Cost Data: The cost provided is an estimate of the hours (100) x \$200/hour rate needed to configure the controller for the demonstration.
- Scalability: Several FRCS would need to be configured, so an incremental increase per device would need to be considered. This is best handled with imaging.

7.3.3 Secure Endpoint

- Description of Cost Element: The Secure Endpoint is the EST-supporting device that would be collocated with remote/end devices that are incapable of PKI.
- Supporting Cost Data: The cost provided is an estimate of the hours (40) x \$200/hour rate needed to configure the controller for the demonstration.

- Scalability: Several endpoints would need to be configured, so an incremental increase per device would need to be considered. This is best handled with imaging.

7.3.4 Installation Costs

- Description of Cost Element: The cost to install the EJBCA PKI Software Appliance can be \$30K+, depending on the scope of the effort (Single environment vs Development or Production implementation). Although it is not a complex process, PrimeKey suggests procurement of installation services for a smooth deployment.
- Supporting Cost Data: Costs are based on prior PrimeKey EJBCA customer implementations.
- Scalability: As mentioned above, the cost for installing the EJBCA PKI Software Appliance can be \$30K+ and will depend on the number of instances deployed.

7.3.5 Maintenance

- Description of Cost Element: The annual maintenance and support cost for the Software Appliance is approximately \$11.5K. This is a required cost for ongoing support of the Appliance.
- Supporting Cost Data: The current commercial cost provided is for an annual maintenance and support services. These include a Customer Support service center, as well as online access to a download site for upgrades and patches.
- Scalability: Costs are for annual maintenance and support per appliance

7.3.6 Hardware Lifetime

- Description of Cost Element:
 - Secure Endpoint: This is an annual replacement cost based on device price estimate replaced every 7 years.
- Supporting Cost Data:
 - Secure Endpoint: Based on the cost of components specified for use in S&C microgrid projects.
- Scalability:
 - Secure Endpoint: This estimate would need to be multiplied by the number of devices deployed (plus spares).

7.3.7 Operator Training

- Description of Cost Element: Per person cost for the Standard EJBCA Open Training class. This week-long class provides training on the installation and operations of the EJBCA PKI.
- Supporting Cost Data: This is the current standard cost per person as offered by PrimeKey.
- Scalability: The cost provided is for one attendee and should be increased accordingly based on the number of attendees.

7.4 COST DRIVERS

There are several cost drivers that should be considered for future implementations. The size of the deployment, types of end devices to be integrated, and level of integration support may significantly impact cost. The following are some examples of how these cost drivers may impact the implementation and operational costs of the technology.

- EJBCA PKI: Costs are easily determined and controlled since the EJBCA PKI Software Appliance is a commercial PKI solution. The cost will vary based on the number of Appliances needed for a specific implementation
- Installation and Integration Services: These costs will need to be evaluated on an implementation-specific basis:
 - End Device Integrations: The cost will be determined by the amount of effort in getting the **end devices** incorporated. Factors include:
 - Number of end devices to be incorporated
 - Types of end devices
 - Number of different types of devices
 - Level of integration services required
 - Manual or automatic certificate enrollment
- Operator Training: FRCS cybersecurity personnel may require training on the EJBCA PKI and GridMaster system solutions, to operate and maintain them daily.

7.5 COST ANALYSIS AND COMPARISON

Ongoing operational costs of the technology is defined and easily determined. There will be an annual Support and Maintenance cost for EJBCA, which will include downloads for upgrades/patches/fixes, as well as access to an extensive knowledge base of EJBCA product information. Additional installation and integration services may be required only if there are additional appliances and end devices to be incorporated into the CRN PKI.

8.0 IMPLEMENTATION CONSIDERATIONS

There are many options to consider for a PKI implementation; the most secure of the available options were chosen for the NREL demonstration. However, in real-world scenarios, the need for high-availability, budget constraints, and other factors may limit the feasibility of some of these choices. Design decisions for a real-world implementation may diverge from the choices made for the demonstration in some of the areas discussed below.

Integration of PKI is facilitated by the EJBCA system, which is a commercial product designed and supported for that purpose, so most implementation considerations of the demonstrated technology will likely center around PKI capabilities of *end devices*. It is necessary to first determine feasibility of interoperability and configuration methods for PKI on devices in the candidate network.

8.1 END DEVICE PKI CAPABILITIES

For the purposes of the demonstration, devices were equipped with the capabilities listed in Table 4 “PKI-Related Capabilities” below. Some of the listed capabilities are not absolutely required for participation in PKI but would allow a device to take full advantage of the provided PKI services, and/or facilitate administration.

Table 4. PKI-Related Capabilities

Capability	Notes
Ability to implement network sockets that support TLS and third-party CA signed certificates.	For the demonstration, sockets were implemented in Java, Python, and by host applications (syslog-ng, etc.).
Support local key and Certificate Signing Request (CSR) generation	Best practice dictates local generation of private key, so that it never leaves the device which uses it. The EJBCA offers alternatives, such as generating a key and certificate remotely, and transporting to the end device.
Setup of temporary credential for initial enrollment of a certificate	This temporary credential should not be stored permanently on the device, requiring a means of making it available temporarily to the device and then removing it.
Support installation and operation of EST client	Configure client to use credentials and perform EST enrollment per RFCs. (RFC 7030 and 8295 define acceptable EST methods). If EST cannot be implemented, EJBCA offers other mechanisms for certificate management (e.g., RESTAPI, ACME, CMP). Manual device certificate enrollments can be performed if no other methods are feasible
Ability to monitor status (e.g., expiration) of current device certificates, report status, and perform automatic renewal	Can be scripted (e.g., cron job/scheduled task) if not a native capability. This capability is required for automatic certificate renewal.
Ability to securely store the private key	The key should be stored as an encrypted file, or within an encrypted file system, and protected with appropriate permissions. Hardware storage is also an option for protecting the private key, which is of paramount importance for the use of PKI.
Ability to report validation errors to centralized location	Required for security monitoring of network and visualization.
Ability to use OCSP or CRL's to validate a peer certificate and its trust chain	Important security component of PKI

The requirements of a specific site- both for security and for ease-of-administration- will determine which of these capabilities need to be made available. For the NREL demonstration, all participating devices were provisioned with these capabilities. The methods used to implement these capabilities for the demonstrated devices are described in Appendix A – Client considerations, Section A.1 “Client-Side Scripting”.

For devices which cannot adequately attain PKI capabilities, “Secure Endpoints” described in Appendix A, Section A.2, could be used to allow the device to participate in local PKI.

8.2 PROTECTING CRITICAL OPERATIONS

An additional concern in PKI implementation is assuring that PKI does not interfere with the essential operations a device performs. This is especially important for industrial networks, which perform critical functions. Although obtaining certificates, renewing certificates, and other PKI functions did not consume excessive bandwidth or processing power on the GridMaster IPC, it was found that rejecting constant invalid connection attempts from a rogue device had the potential to negatively impact performance and interfere with critical GridMaster system functionality. This represents a potential vector for a ‘denial of service’ attack. During testing, this vulnerability was addressed by adding host-based firewall rules which rate-limited connection attempts from a device once it was found to be ‘rogue’. The phenomenon highlighted that an industrial system must remain available to the greatest extent possible, and security controls must be added carefully, *in a way that protects essential functionality*.

Another implementation issue encountered revolved around the persistence of inter-device sessions. Inter-device sessions such as those between GridMaster IPCs may remain connected indefinitely. If one of the device’s certificates is revoked during this session, the revocation would have no effect until the connection is broken and re-established.

One work-around would be to have connections broken at regular intervals via “session timeouts”. However, where availability is critical, interrupting inter-device connections can have serious consequences and needs to be avoided. For the purposes of the demonstration, utilities were added (these were not readily available options on TLS socket libraries in Python or Java) which cached the remote device’s certificate and re-validated it at regular intervals in a separate thread, only breaking the connection if the peer’s certificate had been revoked or was otherwise invalid. The outcome was that revocation had a real-time effect on active device connections, and valid inter-device connections were not broken needlessly for validation checking.

Even if validation checks can be performed without breaking TLS connections, it will be necessary to temporarily disconnect a session to allow for renewal of a certificate (even if the renewal process is automated). On some networks, automatic renewal may need to prompt for administrative confirmation before resetting a critical device connection.

8.3 PKI AUDITING

Monitoring PKI activities and related security events would be a critical feature for a network provisioned with local PKI. Certain PKI events and information, such as certificate status and expiration for a given host, are searchable through the web UI of the EJBCA.

However, PKI implementation also creates a class of auditable events that will be of interest for the operators, and these are not captured by the CA server. These would include instances when an invalid certificate is used to attempt a connection (of security interest), or a host with an expiring certificate is unable to reach the CA to request renewal (which could lead to operational issues). Other security related events may include a device attempting to use a certificate with an incorrect SAN field (perhaps a device's certificate specifies a hostname or IP that differs from what the device is using), or a device is using a client certificate while functioning as a server.

These events would only be captured in the local logs of the end devices themselves, not by the CA. It seems highly advisable to aggregate and structure this data so that it can be easily reviewed. For the NREL demonstration, monitoring included sending PKI and certificate-related logging information to the syslog server, which was able to filter and aggregate this information and provide status data and security alerts. More sophisticated methods may need to be developed for various sites. See A.1.1.4 Notes on Logging for more details.

8.4 CERTIFICATE VALIDATION AND EXPIRATION OPTIONS

8.4.1 Automatic Certificate Revocation

Automatic certificate revocation upon renewal was demonstrated at NREL (after the primary test cases were exercised) showing security advantages to revoking an existing certificate once it has been replaced with a new certificate (and private key). This eliminates an extra, valid key-pair that could be compromised, especially if a device is decommissioned and replaced. This functionality is available through the EJBCA interface. Specifically, the EJBCA CA server was configured to revoke an existing certificate once that certificate was used as a credential to obtain a new one. This configuration and practice would likely be incorporated into future implementations of the technology.

8.4.2 Revocation Checking

The ability to check the status revocation status of a certificate before accepting it is a significant security feature of PKI. For the NREL demonstration, both OCSP and CRLs were used for this purpose. GridMaster IPC connections were configured with the most stringent settings: connections were validated through OCSP with the EJBCA each time they were made and would have been rejected if the OCSP resource was unavailable for validation services. Although this may be considered the most secure choice, this also makes OCSP availability a single point of failure for the entire network. This risk may be unacceptable when availability is an overriding concern.

Other items of note regarding implementation were not so much “issues” as they were choices which had to be determined when implementing a local PKI architecture.

The architect must determine the rigidity and frequency with which OCSP or CRL validation is performed:

- Should a connection be accepted if the OCSP source is unavailable? (Requiring validation from the OCSP source for each connection would make OCSP availability a single point of failure for the network).

- In the case of CRL's, what should happen if CRLs are unavailable or expired? What is the maximum age of a CRL?

The architect must determine properties of the X509 certificates:

- What is the lifetime of certificates? This would be determined on the CA server's settings. Shorter lifetimes may be more secure, as a compromised certificate would expire quickly. However, shorter certificate lifetimes would mandate more frequent certificate renewals, which may disrupt network connections, or cause potential points of failure.

8.5 KEY STORAGE

The use of certificates implies the existence of a private key which must be protected. Storing the key in the filesystem may be necessary, which would mean that if a device is physically compromised and the file system is unencrypted, a malicious actor may be able to obtain the key. There are methods which can encrypt the key (for example an encrypted PKCS12 or Java "Keystore") however these would be limited by the constraints of a typical industrial network: the device must usually be able to start and function without human intervention. Thus, requiring an operator to enter a passphrase, for example, which decrypts the key or the file system at boot-up, would likely *not* be acceptable.

Hardware key storage was beyond the scope of this current project, but hardware methods are available which may help in providing secure key storage.

The immediate workaround, however, would be partially procedural and several methods were identified that could mitigate the risk of a compromised key:

- Use short lifetimes so that certificates (and associated keys) on decommissioned equipment expire rapidly and become unusable.
- Diligently revoke device certificates when decommissioning equipment or sending it away for repair (a procedural method).
- When a certificate is renewed, revoke the device's previous existing certificate, to keep the number of valid certificates in existence to a minimum. This setting is available on the EJBCA, which automates this functionality.
- Use physical and network intrusion monitoring to identify tampering with a device and revoke a device's certificate if key compromise is suspected.

8.6 ACCURATE TIME SOURCE

TLS certificates have an expiration date and a "begin" date and will not be accepted outside that timeframe. This means that all end devices, and the EJBCA itself, will need to be synchronized to an accurate time source. Because CRNs are isolated from internet NTP servers, end devices as well as the EJBCA will need to synchronize to a local time source. A GridMaster IPC (via a GPS dongle) provided this time source at the NREL demonstration, as it can synchronize with GPS satellites and can act as an NTP server.

8.7 UI FOR END DEVICES

Some activities performed on end devices will require active human intervention. For example, a credential is required during initial enrollment to authenticate over EST. Some scripting/programming may be required on these devices to create a user-friendly interface and avoid requiring extensive manual commands or expert knowledge of PKI. The interface may reside on the device itself, as was demonstrated at NREL, or may reside on a remote device which has access to the field device and can install the certificate or run the enrollment commands remotely. For information on the interface developed for this project and used at the NREL demonstration, see Appendix A.

9.0 REFERENCES

- PrimeKey EJBCA architecture <https://doc.primekey.com/ejbca/ejbca-introduction/ejbca-architecture>
- PrimeKey EJBCA internal architecture <https://doc.primekey.com/ejbca/ejbca-introduction/ejbca-architecture/internal-architecture>
- Department of Defense (DoD) Risk Management Framework and Cybersecurity directives, including related Service-specific guidance:
 - DoD Instruction 8500.01, Cybersecurity, March 14, 2014
 - DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017
 - National Institute of Standards and Technology (NIST) 800 series special publications:
 - (NIST) Special Publication (SP) 800-82, Guide to Industrial Control Systems (ICS) Security, Revision 2, May 2015
 - NIST SP 800-60, Information Security, Revision 1, Volumes I & II, Information Security, August 2008
 - NIST SP 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016, Updated June 7, 2018
 - NIST SP 800-53, Revision 5, Security and Privacy controls for Information systems and Organizations, September 2020
 - Whole Building Design Guide (<http://www.wbdg.org/>) publications:
 - Unified Facilities Criteria (UFC) 4-010-06, Cybersecurity of Facility-Related Control Systems, Change 1, January 18, 2017
 - Unified Facilities Guidance Specification (UFGS) 25 05 11, Cybersecurity for Facility- related Control Systems, November 1, 2017
 - Security Technical Implementation Guides (STIG) and Security Requirements Guides (SRG) (<https://public.cyber.mil> or <https://cyber.mil>)
 - Zero-Trust Reference Guide (coming FY2021), collaboration between the Defense Information Systems Agency (DISA), National Security Agency (NSA), U.S. Cyber Command, and the private sector

APPENDIX A CLIENT CONSIDERATIONS

A.1 CLIENT-SIDE SCRIPTING

Although the EJBCA system can provide all needed PKI services to the CA CRN, participation (especially automated participation) requires client-side functionality on the end devices. For the purposes of the NREL demonstration, a utility to facilitate and automate PKI activities on end devices was developed and installed on all the Linux-based devices. The details of the utility are described in further detail below. Since vendors and developers will likely implement proprietary approaches and design their own custom utilities, the following table outlines the functions provided by the NREL utility. Similar functionality will need to be made available to any end devices which will participate in PKI, especially if processes (such as certificate renewal) are automated.

Table 5. Local Functionality for PKI Participation

Functionality	Notes
Device will need to be configured with and store the IP address, or DNS name of the CA (EJBCA)	The IP address or URL to reach the CA server will vary from site to site and would need to be configured. To use EST, the devices need this IP or URL. (See Figure 18)
Trusted certificates need to be installed from the CA server onto the local device. “Trusted Certificates” refer to the root, management, and CA certificates for the local PKI.	This is critical so that each device knows to trust certificates signed by the local trusted root.
Device will need to generate a key-pair and CSR.	Key generation is most secure if the keys (private and public) are locally generated on the device and never leave the device. Generating the keypair locally allows this to occur. If this is impossible, the EJBCA offers the ability to generate keys and certificates for transport to a device.
Devices will need to be able to use a temporary credential for initial enrollment over EST.	Although the process for subsequent renewals can use the device’s valid certificate (and be fully automated), initial enrollment will require a password and username. This should not be stored permanently on the device. (See Figure 19)
Devices will need to install the certificates obtained through EST and restart appropriate services as necessary.	Locations and storage methods for keys and certificates will vary by device-type.
Devices will need to be able to run a scheduled task which checks the expiration status of their device certificate, and renew it when some threshold has passed	This threshold was made user-configurable via the utility. (See Figure 18)
Device should monitor and audit PKI activity, both manual and automated, and report PKI related events and alerts to a centralized location for administration and review.	PKI activities and the use of certificates creates a class of auditable events. (Figure 22, Figure 23)

A.1.1 Utility Used for Client-Side PKI Functions at NREL Demonstration

The NREL demonstration was intended to demonstrate out-of-box configuration for all the devices. This meant that all site-specific configuration, including for the EJBCA and all the end devices, was to be performed as part of the demonstration. A unique root of trust was instantiated onsite on the EJBCA, and all end devices were configured, onsite, to trust the new CA trust chain and to obtain certificates automatically from the issuing CA through EST.

In practice, the demonstration operators at NREL were acting as the onsite administrators of the **local site** (rather than representatives of the OEM): receiving PKI-capable equipment from the OEM and configuring that equipment with all site-specific parameters. To facilitate initial enrollment and site-specific configurations on the Linux hosts (GridMaster IPCs, Secure Endpoints, syslog server) a utility was developed which provided the local devices with the functionality enumerated in Table 5.

A.1.1.1 *Architecture of the Utility*

The utility was packaged as a Debian package and installed at the “factory” (a task which would be performed by an OEM) as part of the baseline image for the devices. The local site admin would be expected to use the utility with a unique account which provided privileges limited to PKI administration (no access to OEM settings, the underlying platform, or any other applications). SSH was selected as the out-of-band management interface, because it is secure, widely available, and does not rely on PKI.

Because SSH was used, a text-based dialog-type menu was chosen to present choices and allow for configuration (see Figure 17 below). This menu structure allowed sufficient ‘ease of use’ for purposes of the demonstration. It is also lightweight and does not draw excessive resources, which is an asset for “Operational Technology” equipment which is usually resource constrained.

To limit the PKI admin’s operations through the utility to only those needed, file system permissions were adjusted to limit the directories accessible to the PKI admin user. Additionally, the “sshd_config” file was configured with the “ForceCommand” parameter. The “ForceCommand” parameter forced the configuration menu (Figure 17) to open immediately upon SSH login for the PKI admin user and prohibited running any other executables other than those spawned by the utility itself. For example, if the user issues ctrl-c to exit the menus, the login will be terminated. The PKI admin user is unable to access the command line which is normally present for SSH sessions.

A.1.1.2 Performing Initial Configuration and Enrollment through the Utility

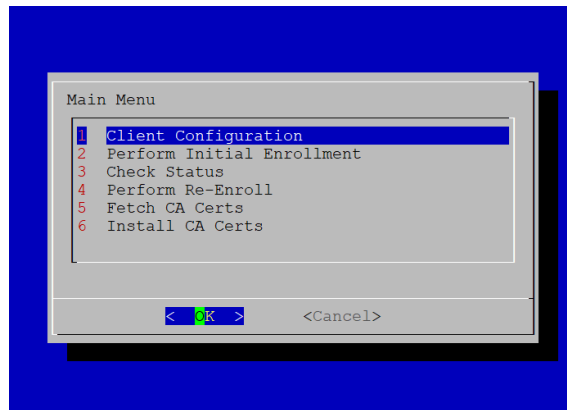


Figure 17. Initial Configuration Menu

The PKI admin user is shown the top-level menu upon successful login over SSH (Figure 17). Using the provided menu, the user can configure the IP address of the CA server, the TCP port to use, and other parameters, such as when to renew a certificate, expressed here in minutes, as this was an accelerated timescale. (See Figure 18 below)

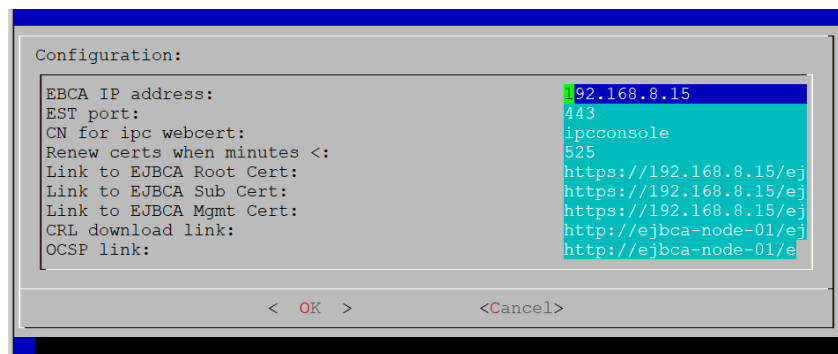


Figure 18. EST Client Settings

The configured parameters are saved and become a part of the device's permanent configuration, as these settings will be used by the automatic renewal process over the lifetime of the device.

After configuring these parameters, the user can fetch and install the trusted certs, and then perform initial enrollment, which would provision the device with a device certificate from the local PKI. For initial enrollment, a credential is required (Figure 19), which was also requested by the utility.

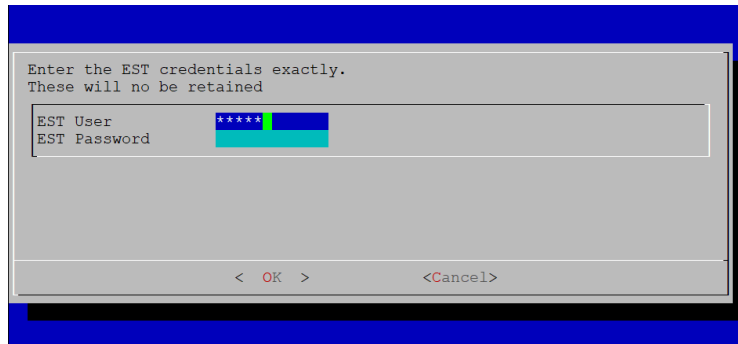


Figure 19. Utility Provides a Means of Entering the Initial Enrollment Credential

Once the credential is entered, the utility generates a keypair and CSR, sends the CSR to the CA server, obtains a device certificate, installs it, and restarts the required services. This is done automatically; success or failure is reported to the user. In the event of a failure (Figure 20), logs are generated (locally and on the EJBCA, Figure 22 and Figure 23) to assist in diagnosing the issue.

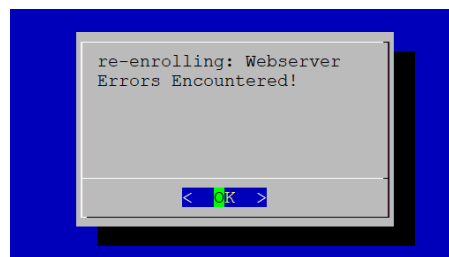


Figure 20. Utility Indicates Success or Failure during Enrollment/Re-Enrollment

A.1.1.3 Notes on Certificate Installation

For the GridMaster IPCs, the certificate's keys are stored in a Java Keystore. The utility replaces the keys in the keystore and restarts the webserver (so that the new certificate will be used). For the syslog server, the keys were stored in protected directories in the filesystem, so the utility places the keys in the proper "PEM" format in the filesystem, applies restrictive file permissions to the keys, and restarts the syslog service. It is important to note that various applications will require various storage formats, various filesystem locations, and possibly require restarting services after certificates are installed. A utility which automates PKI tasks will need to account for these application-specific parameters.

A.1.1.4 Notes on Logging

The use of PKI creates several classes of information that must be audited for security purposes.

A.1.1.4.1 Privileged Actions

Federal CCI's dictate that privileged actions must be logged with sufficient detail. Certainly, PKI operations are privileged, and the client-side utility logged all actions through the interface to the local syslog service (which was forwarded securely to a log aggregator). This includes both user actions (such as initial enrollment) as well as renewal, which was automated.

```

Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:26,135 cert_activity init enrollment activated (user=certadmin)
Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:35,310 cert_activity cert types selected for enrollment are ['Webserver', 'Inter_IPC_Communications',
Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:35,310 cert_activity doing init enrollment on Webserver (user=certadmin)
Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:35,331 cert_activity initialized init enrollment for Webserver (user=certadmin)
Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:35,332 cert_activity running initial enrollment for Webserver (user=certadmin)
Jun 16 17:03:54 192.168.8.10 2021-06-16 17:03:35,333 cert_activity vars: CN for cert: ipconconsole (user=certadmin)

```

Figure 21. Sample Logs for PKI Activities through the Client-Side Utility.

The EJBCA also contains local audit logs which track EST activities as well as configuration changes to the EJBCA server configuration (all of which would be considered privileged activities).

2021-06-17 18:09:33+0000	End Entity Edit	Success	Local admin call from EndEntityManagementSession.decRequestCounter
2021-06-17 18:09:33+0000	Certificate Create	Success	EstOperationsSessionBean - reenroll: CN=192.168.8.10,OU=DoD,OU=Devices,O=U.S. Government,C=US
2021-06-17 18:09:33+0000	Certificate Store	Success	EstOperationsSessionBean - reenroll: CN=192.168.8.10,OU=DoD,OU=Devices,O=U.S. Government,C=US
2021-06-17 18:09:33+0000	Certificate Request	Success	EstOperationsSessionBean - reenroll: CN=192.168.8.10,OU=DoD,OU=Devices,O=U.S. Government,C=US
2021-06-17 18:09:33+0000	Certificate Revoke	Success	EstOperationsSessionBean - reenroll: CN=192.168.8.10,OU=DoD,OU=Devices,O=U.S. Government,C=US

Figure 22. Sample EJBCA Detailed Audit Logging

A.1.1.4.2 Security and Operational Alerts

In addition to user actions, the implementation of X.509 certificates and PKI creates a class of logging for potential security and operational alerts. When a connection attempt is rejected due to certificate errors, this information represents an important alert for security reasons (perhaps a malicious attack is being attempted) or for operational reasons (perhaps a legitimate connection is failing). In either case, it is important to track these events and alert the proper personnel when such an event occurs. Examples of these types of logs are shown in Figure 23.

```

Jun 17 19:47:44 192.168.8.10 ALERT ! REVOKED CERT: serial=13BEB66D92175793BBB3BA59836DA0C1ABF53C3E /tmp/192.168.8.11.pem
Jun 17 19:47:44 192.168.8.10 ALERT !: REVOKED CERT FOUND FROM DEVICE 192.168.8.11
Jun 17 19:47:44 192.168.8.10 LS5:SUCCESS IN WRITING OPEN COMMAND TO LS5

```

Figure 23. Locally Generated Log Entry Showing a Certificate Validation Issue

A.2 SECURE ENDPOINTS

Secure endpoints were designed to test and demonstrate a method for applying PKI abilities to communications with devices that cannot natively use TLS or receive certificates through EST. In the case where a DER or other device can use serial protocols (DNP3, Modbus, etc.) and cannot be co-located securely with a controller, a secure endpoint acts as a serial to Ethernet/TLS converter and encrypts the serial data during transit, as well as authenticating the identity of the remote endpoint before connecting to it. The Secure Endpoints demonstrated at NREL were PKI and EST capable, so these could be administered through the EJBCA and through the utility described in Section A.1.1, offering the same security controls and centralized administration as other devices on the CRN. The conceptual diagram in Figure 24 illustrates the use of Secure Endpoints.

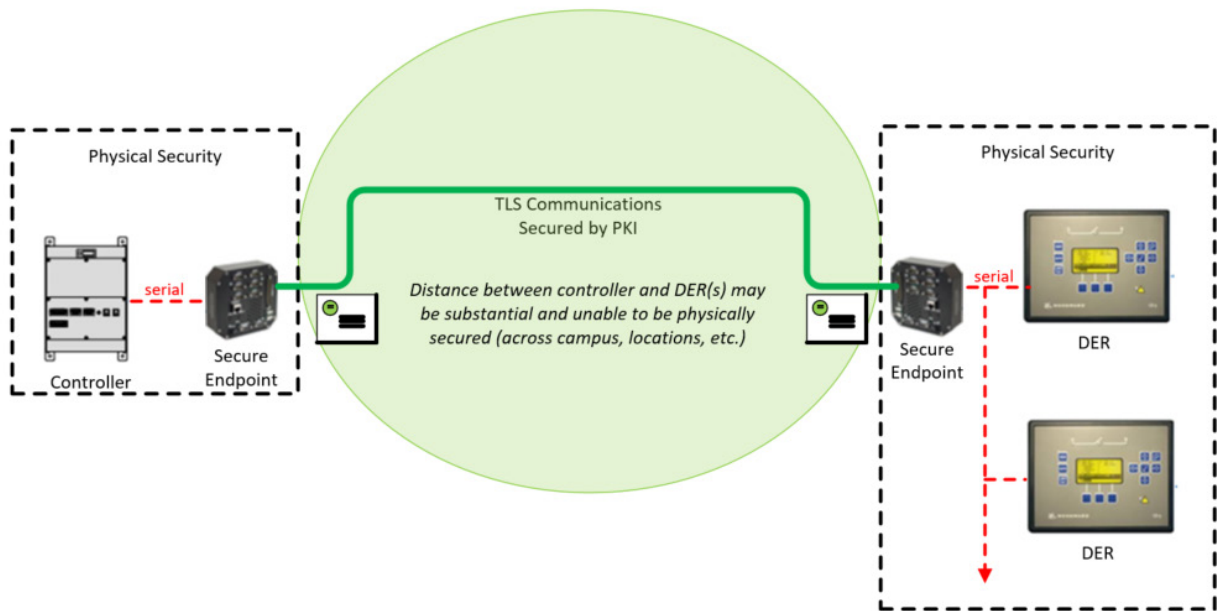


Figure 24. Secure Endpoints Use Case

A.3 OTHER USE CASES

This ESTCP proof of concept focused primarily on leveraging PKI to regulate inter-device connections. However, there are other use-cases for a local PKI on a CRN that would merit exploration.

A.3.1 Signing Site-Created Documents, Files and Recovery Images

The implementation of PKI on a CRN allows the local trust chain to be used to sign and attest to other entities, as well as device certificates. The local PKI instance could be utilized for the issuance of digital certificates used to digitally sign backup images or configuration files used by local devices to restore configurations.

When the recovery file is retrieved from storage and intended to be used for restoration, the signed hash could be used to validate the integrity of the image and assure that it had not been tampered with and was authorized for use.

Logfiles which are archived in storage could also be signed in a similar fashion, and this process used to ensure their integrity when retrieved for analysis.

A.3.2 NTP

NTP is an important factor in CRNs. Unlike internet-connected networks, where time can be synchronized with a variety of online sources, a CRN must provide a local timeserver. With the advent of NTP v4 in the Linux world, X.509 certificates are now supported for authenticating NTP

servers (in place of symmetric keys used in previous versions). It would be possible to use PKI to authenticate trusted NTP servers on the network, which would enhance security and ease administration. The integration of Linux NTP services with public key authentication is described in the “man pages” for version 4 of the NTP daemon, “NTPv4 includes the NTPv3 scheme and optionally a new scheme based on public key cryptography...”. More information about this topic is available online.¹

Cisco Switches:

Cisco devices also support the EST protocol in specific versions of its Internetwork Operating System (iOS)² and would be able to participate in local PKI.

A.3.3 User Authentication

The NREL demonstration primarily focused on inter-device authentication using end-entity certificates. However, user certificates represent another application of PKI. The EJBCA can generate user certificates which could be associated with a local user and used for strong user authentication to CRN resources. This methodology was used during the NREL demonstration for authenticating to the EJBCA server itself.

For example, a user could create a Windows account on the HMI computer and store a user certificate in their user account’s Windows certificate store. When that user attempts to access a network resource, such as a local webserver, the user’s certificate can be leveraged to prove their identity to the webserver, instead of a password.

If added security is desired, the user’s client certificate can be encrypted with a passphrase; in that case even if access to the HMI computer’s filesystem is obtained and the certificate is acquired by an unauthorized individual, the certificate would be encrypted and unable to be used.

Another advantage of user certificates is that they can be centrally managed through the local PKI infrastructure (specifically, through the EJBCA’s administrative web pages). This allows the site administrator to revoke a user’s certificate when that user no longer needs access to the CRN’s resources and would not require logging on individually to each resource and deleting the user’s account (although deleting the account on each device would be part of good cyber hygiene).

¹ https://www.systutorials.com/docs/linux/man/5-ntp_auth/

² https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-est-client-suppl-pki.html

APPENDIX B POINTS OF CONTACT

The following table lists individuals who were involved in this project and the demonstration.

Table 6. Points of Contact

Point of Contact	Organization Name and Address	Phone & E-mail	Role in Project
Linda Gopal	PrimeKey 951 Mariners Island Blvd, #210, San Mateo, CA 94404	408.666.6156 Linda.gopal@primekey.com	PrimeKey Project Manager
Ryan McKinley	PrimeKey 951 Mariners Island Blvd, #210, San Mateo, CA 94404	916.768.9422 Ryan.mckinley@primekey.com	Solutions Consultant, Principal Investigator
Jeff Brooks	PrimeKey 951 Mariners Island Blvd, #210, San Mateo, CA 94404	703.623.8362 Jeff.brooks@primekey.com	Sales Account Executive
Margaret Doty	PrimeKey 951 Mariners Island Blvd, #210, San Mateo, CA 94404	541.842.0961 Margaret.doty@primekey.com	Engagement Director
Aura Lee Keating	S&C Electric Co. 6601 N. Ridge Blvd, Chicago, IL 60626	405.294.3566 auralee.keating@sandc.com	Sr Manager, Cybersecurity Services
Chad Douglas	S&C Electric Co. 6601 N. Ridge Blvd, Chicago, IL 60626	719.453.8553 Chad.douglas@sandc.com	Cybersecurity Analyst
Michael Pinkston	S&C Electric Co. 6601 N. Ridge Blvd, Chicago, IL 60626	972.816.1400 Michael.pinkston@sandc.com	Cybersecurity Architect
Peter Curtiss	S&C Electric Co. 6601 N. Ridge Blvd, Chicago, IL 60626	720.643.9295 Peter.curtiss@sandc.com	Principal Engineer
Christopher Rowland	S&C Electric Co. 6601 N. Ridge Blvd, Chicago, IL 60626	303.848.8798 Christopher.rowland@sandc.com	Cybersecurity Analyst
Brian Miller	National Renewable Energy Laboratory (NREL) 15013 Denver West Pkwy, Golden, CO 80401	303-275-4917 Brian.Miller@NREL.gov	NREL Principal Investigator
John Nangle	National Renewable Energy Laboratory (NREL) 15013 Denver West Pkwy, Golden, CO 80401	303-384-7377 John.Nangle@NREL.gov	Energy Systems Integration Facility (ESIF)
Richard Macwan	National Renewable Energy Laboratory (NREL) 15013 Denver West Pkwy, Golden, CO 80401	303-275-4579 Richard.Macwan@NREL.gov	Network Cybersecurity Recorder
Joshua Rivera	National Renewable Energy Laboratory (NREL) 15013 Denver West Pkwy, Golden, CO 80401	303-384-6931 Joshua.Rivera@NREL.gov	Network Cybersecurity Analyst

APPENDIX C PRIMEKEY EJBCA HARDWARE APPLIANCE

The turn-key PKI hardware solution from PrimeKey is another option to deploy world class PKI in a closed restricted network.

PrimeKey EJBCA Hardware Appliance brings all components needed to successfully deploy and operate a full-blown Public Key Infrastructure (PKI). It includes a complete Certificate Management System, with unlimited number of Certification Authorities (CAs) and/or subordinate CAs, Registration Authority (RA) and a Validation Authority (VA). An integrated FIPS 140-2 Level 3 Certified HSM brings enterprise-grade security keeping all cryptographic keys secure.

Depending on the requirements, PrimeKey offers five hardware appliance models to address different needs. They range from an XS model that is designed to operate as a dedicated root CA to an XL that is suited for extremely large PKI deployments. The models in-between offers variation in the number of certificates and the performance that they can manage. Additionally, the VA and RA can be purchased as separate models. Therefore, PrimeKey EJBCA Appliance is a perfect fit for any PKI deployment.

PrimeKey Appliance Platform comes with a modularized and flexible software stack. PrimeKey Security Foundation Platform (SFP) includes a hardened Linux OS, and all application components are operated as virtual machines which allows for maximum flexibility in the system and simplified procedures for updates or backups.

A dedicated Virtual Gateway (VGW) handles all incoming requests. Central control with a VGW and separation of virtual networks maximizes the security also allowing tight control of the data flow between the interacting software components.

An HSM abstraction layer hides the complexity of the underlying technology and simplifies the integration of software components that require access to the secure hardware.

APPENDIX D PKI AUTHENTICATION STIG REQUIREMENTS

**Windows 10 Security Technical Implementation Guide: Version 2, Release: 2 Benchmark
Date: 04 May 2021**

Vul ID: V-220818	Rule ID: SV-220818r569187_rule	STIG ID: WN10-CC-000115
Severity: CAT II	Classification: Unclass	Legacy IDs: V-63627; SV-78117

Discussion: Using certificates to authenticate devices to the domain provides increased security over passwords. By default, systems will attempt to authenticate using certificates and fall back to passwords if the domain controller does not support certificates for devices. This may also be configured to always use certificates for device authentication.

References

CCI: CCI-000366: The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b

Web Server Security Requirements Guide: Version 2, Release: 3 Benchmark Date: 26 Apr 2019

Vul ID: V-41730	Rule ID: SV-54307r3_rule	STIG ID: SRG-APP-000175-WSR-000095
Severity: CAT II Classification: Unclass		

Group Title: SRG-APP-000175-WSR-000095

Rule Title: The web server must perform RFC 5280-compliant certification path validation.

Discussion: A certificate's certification path is the path from the end entity certificate to a trusted root certification authority (CA). Certification path validation is necessary for a relying party to make an informed decision regarding acceptance of an end entity certificate. Certification path validation includes checks such as certificate issuer trust, time validity and revocation status for each certificate in the certification path. Revocation status information for CA and subject certificates in a certification path is commonly provided via certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses.

References

CCI: CCI-000185: The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

NIST SP 800-53 :: IA-5 (2)

NIST SP 800-53A :: IA-5 (2).1

NIST SP 800-53 Revision 4 :: IA-5 (2) (a)

Web Server Security Requirements Guide: Version 2, Release: 3 Benchmark Date: 26 Apr 2019

Vul ID: V-55945

Rule ID: SV-70199r2_rule

STIG ID: SRG-APP-000033-WSR-000169

Severity: CAT II **Classification:** Unclass

Group Title: SRG-APP-000033-WSR-000169

Rule Title: The web server must enforce approved authorizations for logical access to hosted applications and resources in accordance with applicable access control policies.

Discussion: To control access to sensitive information and hosted applications by entities that have been issued certificates by DoD-approved PKIs, the web server must be properly configured to incorporate a means of authorization that does not simply rely on the possession of a valid certificate for access. Access decisions must include a verification that the authenticated entity is permitted to access the information or application. Authorization decisions must leverage a variety of methods, such as mapping the validated PKI certificate to an account with an associated set of permissions on the system. If the web server relied only on the possession of the certificate and did not map to system roles and privileges, each user would have the same abilities and roles to make changes to the production system.

References

CCI: CCI-000213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

NIST SP 800-53 :: AC-3

NIST SP 800-53A :: AC-3.1

NIST SP 800-53 Revision 4 :: AC-3

Web Server Security Requirements Guide: Version 2, Release: 3 Benchmark Date: 26 Apr 2019

Vul ID: V-56027 **Rule ID:** SV-70281r2_rule **STIG ID:** SRG-APP-000427-WSR-000186

Severity: CAT II **Classification:** Unclass

Group Title: SRG-APP-000427-WSR-000186

Rule Title: The web server must only accept client certificates issued by DoD PKI or DoD-approved PKI Certification Authorities (CAs).

Discussion: Non-DoD approved PKIs have not been evaluated to ensure that they have security controls and identity vetting procedures in place which are sufficient for DoD systems to rely on the identity asserted in the certificate. PKIs lacking sufficient security controls and identity vetting procedures risk being compromised and issuing certificates that enable adversaries to impersonate legitimate users.

References

CCI: CCI-002470: The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.
NIST SP 800-53 Revision 4 :: SC-23 (5)

Authentication, Authorization, and Accounting Services (AAA) Security Requirements Guide: Version 1, Release: 2 Benchmark Date: 24 Jan 2020

Vul ID: V-80925 **Rule ID:** SV-95635r1_rule **STIG ID:** SRG-APP-000175-AAA-000570

Severity: CAT I **Classification:** Unclass

Group Title: SRG-APP-000175-AAA-000570

Rule Title: AAA Services must be configured to only accept certificates issued by a DoD-approved Certificate Authority for PKI-based authentication.

Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used to for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses.

References

CCI: CCI-000185: The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

NIST SP 800-53 :: IA-5 (2)

NIST SP 800-53A :: IA-5 (2).1

NIST SP 800-53 Revision 4 :: IA-5 (2) (a)

Authentication, Authorization, and Accounting Services (AAA) Security Requirements Guide: Version 1, Release: 2 Benchmark Date: 24 Jan 2020

Vul ID: V-
80927

Rule ID: SV-
95637r1_rule

STIG ID: SRG-APP-000175-AAA-
000580

Severity: CAT I **Classification:** Unclass

Group Title: SRG-APP-000175-AAA-000580

Rule Title: AAA Services must be configured to not accept certificates that have been revoked for PKI-based authentication.

Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used to for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses.

References

CCI: CCI-000185: The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

NIST SP 800-53 :: IA-5 (2)

NIST SP 800-53A :: IA-5 (2).1

NIST SP 800-53 Revision 4 :: IA-5 (2) (a)