CertAgent v7.0 Patch Level 9

Guidance for Common Criteria Evaluation

Software Version: 7.0 patch level 9.9

Document Version: 2.7.2

Issue Date: July 26, 2023

Authors: Jonathan C. Schulze-Hewett, Pauline Tang

Abstract: This document is the Common Criteria Guidance for Information Security Corporation's CertAgent, Version 7.0 patch level 9.9.

Legal Notice

Use of CertAgent is subject to the terms of your license agreement with Information Security Corporation.

CertAgent is a registered trademark of Information Security Corp. Other product and company names mentioned in this document may be the trademarks of their respective owners.

Document History

Version	Date	Change	Author(s)
1.0.0	2017-08-08	Initial draft document	Pauline Tang
2.0.0	2018-03-15	Revised per NIAP validators comments and updated to comply with final draft version 2.1 of the protection profile	Jonathan Schulze-Hewett, Pauline Tang
2.1.0	2018-03-23	Updated based on lab feedback	Pauline Tang
2.2.0	2018-03-26	Updated based on lab feedback	Pauline Tang
2.2.1	2018-03-29	Added TOE Guidance section	Pauline Tang
2.2.2	2018-05-04	Updated based on lab feedback	Pauline Tang
2.2.3	2018-05-22	Updated based on lab feedback	Pauline Tang, Jonathan Schulze-Hewett
2.2.4	2018-05-28	Updated based on lab feedback	Pauline Tang
2.2.5	2018-05-28	Updated based on lab feedback	Pauline Tang
2.2.6	2018-06-21	Updated based on lab feedback	Pauline Tang
2.2.7	2018-06-25	Updated based on lab feedback	Pauline Tang
2.3.0	2018-07-05	Updated based on lab feedback	Pauline Tang
2.4.0	2019-07-15	Updated based on TOE update	Pauline Tang
2.5.0	2020-01-08	Updated based on TOE update	Pauline Tang
2.6.0	2020-09-15	Updated based on TOE update	Pauline Tang
2.6.1	2020-11-19	Updated based on TOE update	Pauline Tang
2.6.2	2021-06-29	Updated based on lab feedback	Pauline Tang
2.6.3	2021-07-27	Updated based on ECR comment	Pauline Tang
2.7.0	2022-01-05	Updated based on TOE update	Pauline Tang
2.7.1	2022-04-06	Updated based on TOE update	Pauline Tang
2.7.2	2023-07-26	Updated based on TOE update	Pauline Tang

Table of Contents

1. Overview

1.1 Purpose

The purpose of this document is to describe how to install, configure, run, and maintain the CertAgent in NIAP-compliance mode. It also provides guidance specified in the “Protection Profile for Certification Authorities” document for evaluators to evaluate CertAgent.

1.2 Scope

The guidance in this document is limited to only those areas related to the secure operation of CertAgent as defined in the “Protection Profile for Certification Authorities”.

The major TOE components in the evaluated configurations are CertAgent, Apache Tomcat, and ISC CDK.

1.2.1 CertAgent 7.0

CertAgent, the TOE, is an X.509-compliant certificate authority (CA). It is an easily managed, web-based certificate authority (CA) intended to be used as the core component of an enterprise public key infrastructure (PKI). Designed to meet the needs of a wide variety of organizations, the current release offers enhanced enrollment services (EST), remote administration, integrated certificate and CRL database, and an OCSP responder. It supports an unlimited number of root and intermediate CAs, providing support for as complex a certificate hierarchy as the size of the enterprise warrants.

CertAgent version 7.0 patch level 9.9 (a.k.a 7.0.9.9) is used for testing.

1.2.2 Apache Tomcat 8.5.91

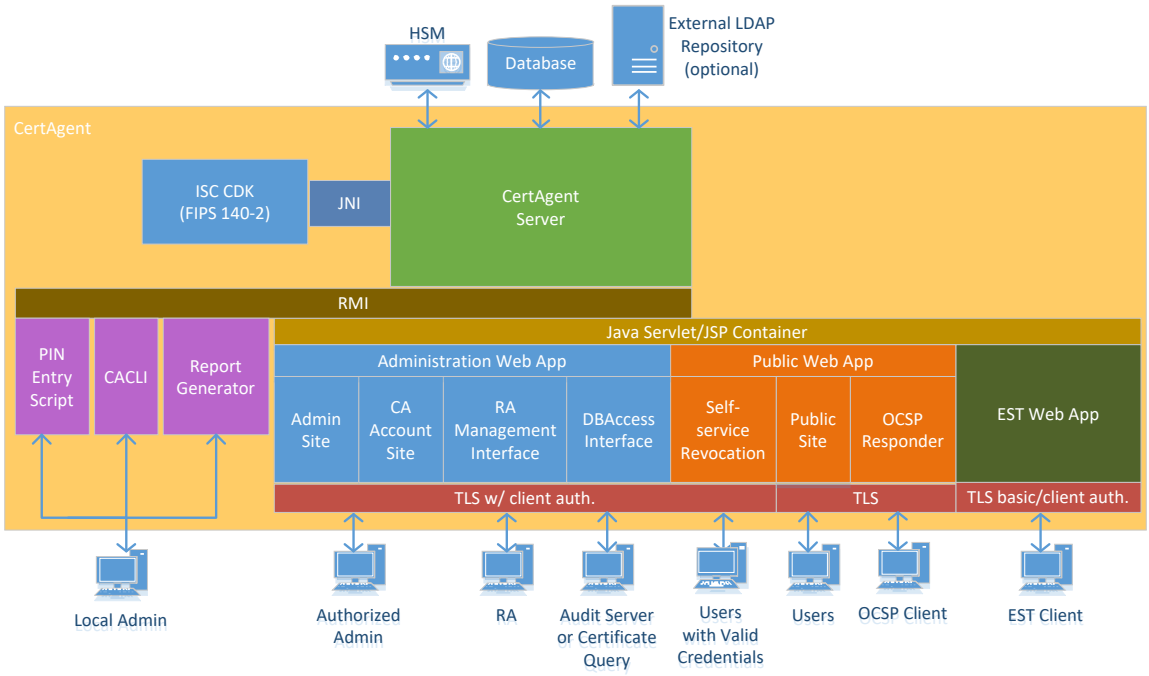
Apache Tomcat application server that hosts the CertAgent web application and the web interface. In the evaluated configuration Apache Tomcat is configured to use the ISC CDK and the PKCS#11 Cryptographic Module for cryptographic operations. Apache Tomcat is part of the TOE’s installation package and is installed when CertAgent is installed.

1.2.3 ISC Cryptographic Development Kit 8.0

The TOE uses ISC’s Cryptographic Development Kit (ISC CDK) for many of the cryptographic operations. The ISC CDK is a shared library to which the CertAgent web application and Apache Tomcat are linked dynamically.

1.3 CertAgent Architecture

The following diagram illustrates the basic layout of the CertAgent system.



The CertAgent 7 System Architecture

1.4 Interfaces

Most CA activities are completed by using a web browser or other tool that connects to the CertAgent web interface and service. The CA supports seven web-based interfaces using different ports or URLs (Admin Site, CA Account Site, Public Site, RAMI (Registration Authority Management Interface), DBAccess, EST, and OCSP) and command line tools.

Below table describes the available web interfaces:

Web Interface	Description
Admin Site	This interface requires valid identification and authentication credentials in the form of certificates. It is secured using client authenticated HTTPS/TLS. Only Administrators and Auditors can access this interface.
CA Account Site	This interface requires valid identification and authentication credentials in the form of certificates. It is secured using client authenticated HTTPS/TLS. Only Administrators, Auditors, and CA Operations Staffs can access this interface. Their responsibilities are described in the next section.
Public Site	This interface is secured using HTTPS/TLS and HTTP. All pages except the CA Information page are HTTPS/TLS protected. The CA information page, used by relying parties to obtain CRLs, issuer certificates, and CA version information, is available without security over HTTP.

	All pages except the self-service revocation page are unauthenticated. The self-service revocation page requires valid identification and authentication credentials in the form of certificates. Unauthenticated users can submit certificate requests, enroll via the browser, retrieve or install their certificates, search for certificates, and view and download CA's certificate and CRL.
Registration Authority (RAMI)	This interface requires valid identification and authentication credentials in the form of certificates. It is secured using client authenticated HTTPS/TLS. Only CA Operations Staffs with 'RAMI' permission can access this interface. Their responsibilities are described in the next section.
DBAccess	This interface requires valid identification and authentication credentials in the form of certificates. It is secured using client authenticated HTTPS/TLS. Only Administrators, Auditors, and CA Operations Staffs with 'DBAccess' permission can access this interface. Their responsibilities are described in the next section.
EST	This interface requires secured using HTTPS/TLS. Subscribers who are authenticated with either certificates or their name and password can submit an enrollment request to obtain a certificate. Unauthenticated users can obtain the CA's certificate via this interface.
OCSP	This interface is available without security over HTTP or secured using HTTP/TLS. All accesses are unauthenticated. Users can use this interface to obtain the revocation status of a certificate.

TABLE 1 WEB INTERFACES

Only users who hold an administrator role in the TOE are allowed to have administrator privileges on the physical system on which the TOE is installed. Below table describes the command line tools they can execute from the local console of the physical system.

Tool	Description
CertAgent Script certagent.[bat|sh]	Start/Stop CertAgent service, inject the PKCS#11 Cryptographic Module PIN to unlock the "System" credential's private key
Database Script hsqldb.[bat|sh]	Start or stop HyperSQL database
Set PIN Script setpin.[bat|sh]	Inject the PKCS#11 Cryptographic Module PIN to unlock the "System" credential's private key
CACLI cacli.[bat|sh]	Create/Disable CA accounts, manage CA account's credential, manage profiles, manage account/profile configuration, manage ACLs, and manage trust anchor list and CRLs for path validation.
Report Generator reportgenerator.[bat|sh]	Generate certificate status reports
Update Tool update-tool.[bat|sh]	Check for updates, validate the update package, and install the update package.

TABLE 2 COMMAND LINE TOOLS

1.5 Privileged User Roles

The TOE is managed by authorized administrators using a web user interface and the local console as needed. All certificate related administrative actions are performed via the web interface. The TOE supports three roles (Administrator, Auditor, and CA Operations Staff), each of which consists of an access control list (ACL) of one or more X.509 certificates and one or more rights (admin, audit, certify, revoke, RAMI, and DBAccess).

Only users who hold an administrator role in the TOE are allowed to have administrator privilege on the physical system on which the TOE is installed. They can:

- Inject the PKCS#11 Cryptographic Module PIN to unlock the "system" private key
- Start/Stop the TOE and the Database
- Run the CACLI program (allows the scripting of the creation of a root or issuer)
- Run the Report Generator Program
- Run the update tool (to check for updates or apply updates to the system)

The CertAgent Administrative webpages, known as the Admin Site, support the following roles and responsibilities:

Role	Permission	Responsibility
Administrator	admin	manage "system" credentials, database configuration settings, manage CA accounts, manage ACLs, trust anchor database, CRL store for path validations, NIAP configuration, run integrity tests, configure audit trails, and manage jobs
Auditor	audit	view and export audit trails

TABLE 3 ADMIN SITE ROLES AND PERMISSIONS

The CertAgent CA Account webpages, known as the CA Site, support the following roles and responsibilities:

Role	Permission	Responsibility
Administrator	admin	manage account configurations (issuer credential, certificate profile, CRL issuance, certificate issuance, EST, OCSP, RAMI, and enrollment options)
Auditor	audit	view and export audit trails, and search certificates
CA Operations Staff	certify	issue certificates, reject invalid certificate requests, manage EST subscribers, manage automated certificate issuance option, and manage RAMI enrollment setting
	revoke	revoke certificates, issue CRLs, manage self-service certificate revocation option, manage automated CRL issuance option, manage RAMI CRL issuance, and revocation settings

TABLE 4 CA SITE ROELS AND PERMISSIONS

The RA Management interface (RAMI) supports the following role and responsibilities:

Role	Permission	Responsibility
CA Operations Staff	RAMI	enroll a certificate, revoke a certificate, reinstate a certificate, issue a CRL, retrieve the CA account information, query certificate/request information, and retrieve an issued certificate

TABLE 5 RAMI ROLE AND PERMISSION

The DBAccess service supports the following roles and responsibilities:

Role	Permission	Responsibility
Administrator of the Admin Site	admin	retrieve CA account name, and subject DN of the CA's current certificate
Auditor of the Admin Site	audit	retrieve the audit trail records of the Admin Site
Auditor of the CA Site	audit	Retrieve the audit trail records of a CA account
CA Operations Staff	DBAccess	query the certificate table, create or drop an index on the certificate table, query the index information of the certificate table, and update the contact email addresses that are associated with the certificate records

TABLE 6 DBACCCESS ROLES AND PERMISSIONS

1.6 Mode of Operation

The TOE supports two modes of operations.

Mode	Description
NIAP	The TOE is running in this mode if it is not started with the maintenance option, and all the NIAP conformance options are enabled. All interfaces are available.
Maintenance	The TOE is running in this mode if it is started with the maintenance option. The data integrity, certificate and path validations, and security role restriction settings are disabled. Only Admin Site is available.

TABLE 7 MODE OF OPERATION

For details on managing the TOE in a different mode, see section *4.1 Starting and Stopping the Service.*

1.7 TOE Guidance

The TOE includes the following guidance documents:

- CertAgent Administrator Guide, version 7.0, July 26, 2023
- CertAgent Installation, Configuration and Management Guide, version 7.0, July 26, 2023
- CertAgent Certificate Authority Guide, version 7.0, July 26, 2023
- CertAgent Public Site Guide, version 7.0, July 26, 2023
- CertAgent Guidance for Common Criteria Evaluation, version 2.7.2, July 26, 2023
- CertAgent 7.0.9.9 Release Notes, July 26, 2023

2. System Requirements

The following sections list components and applications in the environment that the TOE relies upon to function properly.

The TOE does not include the operating systems or hardware of the systems on which it is installed. It also does not include the third-party software required for the TOE to run. Below tables list the software components required by the TOE in the evaluated configurations. The Operational Environment components should be maintained such that the latest security fixes for each component are installed in a timely manner.

Warning: Use of the platform, database, Java, or PKCS#11 Cryptographic Module specified in the table below have not been evaluated as part of the CertAgent TOE.

Warning: Use of other platform, database, Java, or PKCS#11 cryptographic module was not evaluated nor tested during the CC evaluation of the TOE.

Component	Requirement
Server OS	Windows Server 2016
OS Type	64-bit
Database	HyperSQL Version 2.5.1
Java JRE	Oracle Java 11.0.8
PKCS#11 Cryptographic Module	Thales Luna USB HSM model G5 PW-AUTH CL; firmware version 6.24.7

TABLE 8 OPERATIONAL ENVIRONMENT SOFTWARE REQUIREMENTS (WINDOWS)

Component	Requirement
Server OS	CentOS 7.8 w/rng-tools package
OS Type	x86_64 (64-bit)
Database	PostgreSQL Version 11.9
Java JRE	Oracle Java 11.0.8
PKCS#11 Cryptographic Module	Thales Luna USB HSM model G5 PW-AUTH CL; firmware version 6.24.7

TABLE 9 OPERATIONAL ENVIRONMENT SOFTWARE REQUIREMENTS (LINUX)

In addition to the server requirements, a web browser is required for any system to remotely access the TOE (or to access certain functionality when logged into the Operating System in which the TOE is

running). In the evaluated configuration, the TOE was tested using Firefox ESR version 68, and the compatibility of other browsers was not assessed.

2.1 Platforms

Windows Server 2016 x64 and CentOS 7.8 will be used in the evaluation. On CentOS system, its CPU is required to support RDRAND instruction. Run the following command to test if your CPU supports it:

```
cat /proc/cpuinfo | grep –i rdrand
```

Users with administrator privileges to the physical system must be created and used to install the TOE.

2.1.1 Creating Privileged Users

The TOE requires that the environmental Operating System maintains the Operational Environment (OE) Administrator role and the Operational Environment (OE) Auditor role. Members of the OE Administrator role shall be granted root/administrator permissions in the Operating System. On Linux, members of the OE Auditor role shall be placed in an audit group and must not be granted root/sudo permissions. On Windows, members of the OE Auditor role are normal users and must not be granted administrator permissions. Only members of OE Administrators or OE Auditors may access the environmental Operating System. Below sections describe how to generate users and assign roles. Throughout this document, “OE Administrator” and “OE Auditor” will be used to refer to the user with the Administrator and Auditor role respectively.

2.1.1.1 Windows

1. Login to the Operating System as an Administrator of the Operating System.
2. To create an OE Administrator, run the following commands in a command prompt:

```
net user /add <username> <password>
net localgroup administrators <username> /add
```

3. To create a normal user (OE Auditor), run the following commands:

```
net user /add <username> <password>
```

NOTE: The normal user can view the event log, but cannot run the CertAgent’s command line tools (they are restricted by the installer).

2.1.1.2 CentOS

1. Login to the Operating System as root.
2. To enable wheel group as sudoers:

a. Run the 'visudo' command.

b. Uncomment the line with the wheel group that requires a password by removing the highlighted # character.

```
## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
```

c. Save the file and close your editor.

3. To create sudo user (OE Administrator), run the following commands:

```
adduser <username>
passwd <username>
usermod –aG wheel <username>
```

4. To create an auditor group, run the following command:

```
groupadd ca_audit
```

5. To create an OE Auditor, run the following commands:

```
adduser <username>
passwd <username>
usermod –aG ca_audit <username>
```

2.2 Additional Hardware

Certain functions (EST, OCSP, RAMI, DBAccess, and others) will be performed by using a client system that connects to the TOE.

2.3 CentOS Configuration

2.3.1 Random Number Generator

On CentOS, the `rngd` daemon must be running to ensure that `/dev/random` has sufficient entropy. Otherwise, CertAgent cannot be run or there may be long delays during key generation. Follow the steps below to install and configure this daemon.

1. If `rngd` daemon has not been installed, run the following command:

```
yum install rng-tools
```

2. The program `rgnd` and its service will be installed.

3. To start the service and make it starts and stops automatically upon system start-up and shut-down, run the following commands:

```
systemctl start rngd
systemctl enable rngd
```

2.3.2 Uninstalling SSH

Remote access to the Operating System via SSH is excluded from the evaluation. Only authorized users with an Administrator or Auditor role can manage the TOE locally. Run the following commands to disable and remove SSH from the Operating System.

```
systemctl stop sshd
systemctl disable sshd
yum remove openssh-server
```

2.4 PKCS#11 Cryptographic Module

For the evaluation, a Thales Luna USB Password-Authenticated HSM will be used. The Luna client program version 6.3.0 is required to be installed and configured so that the HSM is operating in FIPS 140-2 mode prior to installing CertAgent.

2.4.1 Verifying the Firmware Version

The HSM used during evaluation must be FIPS 140-2 certified. Certification details for the Luna USB HSM Cryptographic Module (Certificate #3210) can be obtained from the following URL:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3210

To verify the firmware version:

1. Run the `lunacm` tool:

   `/usr/safenet/lunaclient/bin/lunacm` (CentOS)

   `C:\Program Files\SafeNet\LunaClient\lunacm` (Windows)

2. The HSM information (slot number, label, serial number, model, firmware version, configuration, and status) will be displayed.
3. Make sure the firmware version matches the one specified in the vendor's validation certificate: 6.24.6 or 6.24.7.

2.4.2 Initializing the Luna USB HSM

To initialize the Luna USB HSM:

1. Run the `lunacm` tool:

   `/usr/safenet/lunaclient/bin/lunacm` (CentOS)

   `C:\Program Files\SafeNet\LunaClient\lunacm` (Windows)

2. Run the following command to initialize the HSM:

```
hsm init –label <label> -domain <domain>
```

For example:

```
hsm init -label Luna1 -domain infoseccorp
```

3. Type ‘proceed’ when prompted and enter the passwords for the Security Officer (SO).

2.4.3 Updating the HSM Policy

By default, the HSM is not running in FIPS 140-2 approved operation mode. Follow these steps to update the HSM policy.

1. Run the `lunacm` tool.

   `/usr/safenet/lunaclient/bin/lunacm` (CentOS)

   `C:\Program Files\SafeNet\LunaClient\lunacm` (Windows)

2. Run the ‘`hsm showinfo`’ command to view the HSM information. The message “*** The HSM is NOT in FIPS 140-2 approved operation mode. ***” indicates the HSM mode.
3. Run the ‘`hsm showPolicies`’ command to show the HSM policies. Locate the “Allow non-FIPS algorithms” configuration in the HSM Policies section.

   For example:

```
HSM Policies
...
     12: Allow non-FIPS algorithms : 1
```

4. Run the following commands to login as the Security Officer (SO) and disable the non-FIPS algorithms in policy #12:

```
lunacm:>role login –name SO
lunacm:>hsm changeHSMPolicy -policy 12 -value 0
```

5. Type '`proceed`' to continue.
6. Run ‘`hsm showinfo`’ command. The message “*** The HSM is in FIPS 140-2 approved operation mode. ***” should now appear.

2.4.4 Creating a User Partition

1. Run the `lunacm` tool.

   `/usr/safenet/lunaclient/bin/lunacm` (CentOS)

   `C:\Program Files\SafeNet\LunaClient\lunacm` (Windows)

2. Run the ‘`role login –name SO`’ command and enter the Security Officer password.

3. Then, run the '`partition create -label <label> -domain <domain>`' command to create a user partition. A password that differs from the SO's password should be entered when prompted.

NOTE: The password and label generated for the user partition will be used by the TOE to access the HSM.

2.4.5 Enabling RSA key generation

If the HSM is operating in FIPS mode, RSA key generation (`CKM_RSA_PKCS_KEY_PAIR_GEN` mechanism) is disabled by default. RSA key generation must be enabled prior to installing CertAgent.

To enable RSA key generation on Windows:

1. Open the configuration file: `C:\Program Files\SafeNet\LunaClient\Crystoki.ini`.
2. Insert the "RSAKeyGenMechRemap=1" setting in the [Misc] section.

```
...
[Misc]
RSAKeyGenMechRemap=1
ToolsDir=C:\Program Files\SafeNet\LunaClient\
...
```

To enable RSA key generation on CentOS:

1. Open the configuration file: `/etc/Chrystoki.conf`.
2. Insert the "RSAKeyGenMechRemap=1;" setting in the Misc section.

```
...
Misc = {
   RSAKeyGenMechRemap=1;
   PE1746Enabled = 0;
...
```

2.5 Database

PostgreSQL Version 11.9 and HyperSQL Version 2.5.1 databases will be used in the evaluation. HyperSQL server and its JDBC driver are included in the CertAgent installation package and will be installed and configured automatically if selected. If PostgreSQL database is used, it is required to be installed along with its JDBC driver prior to installing CertAgent.

2.5.1 Installing PostgreSQL 11.9

If you do not already have the PostgreSQL server installed, it may be downloaded for free from PostgreSQL webpage:

`https://www.postgresql.org/download/`

See the vendor's documentation for installation and configuration instructions.

2.5.2 Installing PostgreSQL JDBC Driver

If you do not already have the PostgreSQL JDBC driver installed, it may be downloaded for free from the PostgreSQL webpage:

`https://jdbc.postgresql.org/download.html`

To install, choose the appropriate JDBC driver according to your PostgreSQL database version and save it to a file. JDBC 4.2 Driver Version 42.2.16 will be used in the evaluation.

When the CertAgent installer prompts for the JDBC path, specify the location of the JDBC driver file.

Warning: The JDBC library provided by PostgreSQL maintains several copies of the password in memory. ISC has created a modified version of that JDBC driver that corrects this issue. This JDBC driver can be downloaded from ISC's website and should be used by the TOE to establish database connection to PostgreSQL database.

2.5.3 Creating a Database User

A database user is required to have its own database schema to store CertAgent tables. Log in to the PSQL program as a system user and run the following commands to create a new database and a new user for CertAgent.

NOTE: The schema name must be exactly the same as the user name, and the password must be wrapped in single quotes.

```
Syntax:
sudo su – postgres
createdb <db name>
psql –d <db name>
create user "<user>" password '<password>';
create schema "<schema>" authorization "<user>";

Example:
sudo su – postgres
createdb certagentdb
psql –d certagentdb
create user "certagent" password 'password';
create schema "certagent" authorization "certagent";
```

The above database name, user, and password information are required when configuring the database settings in the installer. Please pass this information to the local administrator.

2.5.4 Using JDBC URL

To configure the CertAgent host to use the thin driver for database access, specify a database URI of the following form:

`jdbc:postgresql://<host>:<port>/<database>`

The above URL is required when configuring the database settings in the installer. Please pass this information to the local administrator.

2.6 Java

A 64-bit Java 8 (also known as 1.8.0), 11, or above is required to be installed independently before installing the TOE. Oracle JDK/JRE, OpenJDK, Amazon Corretto, and AdoptOpenJDK are supported. Oracle Java version 11.0.8 will be used in the evaluation.

For the client system accessing the TOE API remotely, Oracle JDK 8, 11, or above is required to compile and run the Java program. The latest version of Java can be downloaded from the following Oracle webpage:

`https://www.oracle.com/java/technologies/javase-downloads.html`

2.7 Servlet Container

A servlet container is required for CertAgent to run the web applications. Tomcat 8.5.91 will be used in the evaluation. It is included in the CertAgent installation and will be installed and configured automatically during the installation.

2.8 Web Browser

A web browser is required for any system used to administer the CertAgent web interface. Firefox ESR version 68 will be used and is required to be installed before or after the CertAgent installation.

Firefox can be downloaded from the following Mozilla webpage:

`https://www.mozilla.org`

2.9 Firewall

The TOE should be installed on a machine that is well-protected behind a properly configured firewall. In particular, only the following ports should be opened to the host system:

- the Admin and CA Account Sites' port for HTTPS with client authentication (default: 8443)
- the Public Site's port for HTTPS without client authentication (default: 443)
- the HTTP port (default: 80) to accept OCSP requests

The following ports are used by the TOE and are restricted to local access by default.

- the database listening port (default: 9001 for HyperSQL and 5432 for PostgreSQL)
- the RMI port (default: 1099)
- the Tomcat shutdown port (default: 8117)

To configure the firewall on CentOS:

1. Login to the system as root.
2. Select System, Administration, Firewall from the menu bar.
3. Enable the Firewall if it has been disabled.
4. Select **Trusted Services** from the left panel.
   a. Check 'WWW (HTTP)' and 'Secure WWW (HTTPS)' to enable ports 80 and 443.
   b. Uncheck 'SSH' if it is enabled.
5. Select **Other Ports** from the left panel.
   a. Click **Add**.
   b. Check 'User Defined'**.**
   c. Enter '8443' in the Port/Port Range field and click **OK**.
6. Check all existing configurations to make sure these ports are not opened: 9001/5432, 1099, and 8117.
7. Click **Apply** to apply the changes.

To configure the firewall on Windows:

1. Login to the system as Administrator.
2. Run 'WF.msc' command to open the Windows Firewall with the Advanced Security dialog.
3. Enable the Firewall if it has been disabled.
4. To open the required ports:
   a. Select **Inbound Rules** from the left panel, and then click **New Rule** in the Actions panel.
   b. Select **Port**, and then click **Next.**
   c. Select **TCP**, enter '80,443,8443' in the specific local ports field, and then click **Next**.
   d. Select **Allow the connection**, and then click **Next**.
   e. Check **Domain**, uncheck **Private** and **Public**, and then click **Next**.
   f. Enter a name for this rule (e.g. CertAgent ports), and then click **Finish**.
5. Check all existing inbound rules to ensure these ports are not opened: 9001/5432, 1099, and 8117.

3. Installation

3.1 Download

TOE installation packages are delivered in a zipped archive via ISC's website. A valid account on our website is required to download the package, and a serial number is required to install the TOE. The software and serial number are delivered over HTTPS.

Warning: CertAgent installation package includes two installation options: NIAP compliance and non-NIAP compliance. In the evaluation, CertAgent will be installed with the NIAP compliance option and configured with strict NIAP conformance settings which fulfill the SFRs. Installing CertAgent in non-NIAP compliance option or disabling the NIAP conformance settings will not be evaluated nor tested during the CC evaluation of the TOE. For details on NIAP compliance settings, see section 4.4.2 Managing NIAP Conformance Settings.

Warning: CertAgent's OCSP capability is divided into basic OCSP support and enhanced OCSP support. Basic OCSP support provides OCSP responses for issuers managed by the CertAgent instance. If enabled, enhanced OCSP support, known as Dhuma, provides OCSP responses for issuers not managed by the CertAgent instance. The evaluated configuration enabled enhanced OCSP support but operating the TOE with basic OCSP support is considered equivalent.

Warning: The JDBC library provided by PostgreSQL maintains several copies of the password in memory. ISC has created a modified version of that JDBC driver that corrects this issue. This JDBC driver can be downloaded from ISC's website and should be used by the TOE to establish database connection to PostgreSQL database.

3.2 Installation

The following information may be prompted for during the installation process. A description for each field is found in the table below:

Field	Format and Description
Installation Type	NIAP compliance or non-NIAP compliance
64-bit Java installation directory	64-bit Java installation directory; e.g., /usr/java/jdk-11.0.8
Hostname or IP address	Hostname of IP address of the system; e.g., 192.198.0.20
Port number for public HTTPS access (<public port>)	This port will be used for HTTPS without client authentication; default to 443
Port number for admin HTTPS access (<admin port>)	This port will be used for HTTPS with client authentication; default to 8443
Public HTTP option	Option to open an HTTP port for OCSP and CRL retrieval; default: enable
Port number for public HTTP	Prompt if 'public HTTP port' option is selected; This port will be used for OCSP and CRL

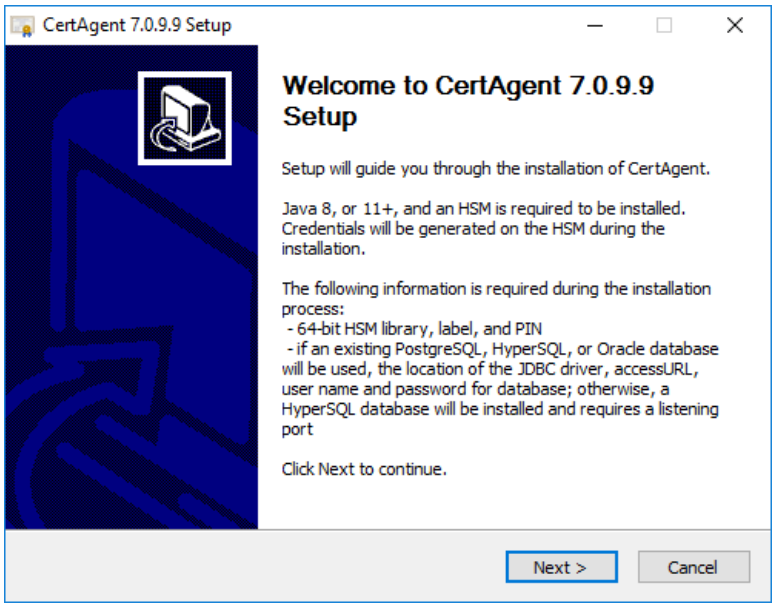
port	retrieval in additional to the public HTTPS access port; default to 80
Installation option	Activate or evaluate the products; default to activate
Product option	CertAgent only Dhuma only CertAgent and Dhuma
CertAgent serial number	CertAgent serial number
Dhuma serial number	Dhuma serial number
Database option	Install and configure a HyperSQL 2.5.1 Use an existing PostgreSQL database Use an existing Oracle database Use an existing HyperSQL database
Port number for HyperSQL database server	Prompt if 'Install and configure a HyperSQL database' option is selected; this port will be used for accessing the HyperSQL database; default to 9001
Password for the default SA account	Prompt if 'Install and configure a HyperSQL database' option is selected; the HyperSQL server is managed by the default SA account. This password will be set for the SA account
Database URL	Prompt if 'Use an existing database' option is selected; database access URL
Database user name	Database user name; If 'Use an existing database' option is selected; user name to manage the 'certagent' database created in the HyperSQL server; default to certagent Otherwise: user name of the existing database
Database user password	Password of the specified database user name
64-bit HSM library	Path of the 64-bit HSM library; e.g., /opt/acala/libacala.so
HSM Partition	HSM Partition; Prompt to select one of the partition found in the HSM
HSM PIN	HSM PIN
Password for credentials (<p12 password>)	PKCS#12 password for TLS and administrator credentials that will be generated by the installer
Organization	Organization; e.g., ISC. If prompts, this value will be used to populate the subject DN base: O=<organization>, C=US
Subject DN base (<base>)	Subject DN base; e.g., O=ISC, C=US. This value will be used to populate the subject DN of the initial certificates; <dn>: <prefix>, <base>
Subject DN Prefix (<prefix>)	Subject DN prefix; e.g. CN=CertAgent 7.0.9 Root CA E275; This value will be used to populate the subject DN of the initial certificates; <dn>: <prefix>, <base>
Validity Period	Validity period for the initial certificate
Key type	Key type of the initial certificate; Select either RSA 3072 or NIST P-384
DN encoding	DN encoding for the initial certificate; PrintableString (default) or UTF8String

TABLE 10 INSTALLATION OPTIONS

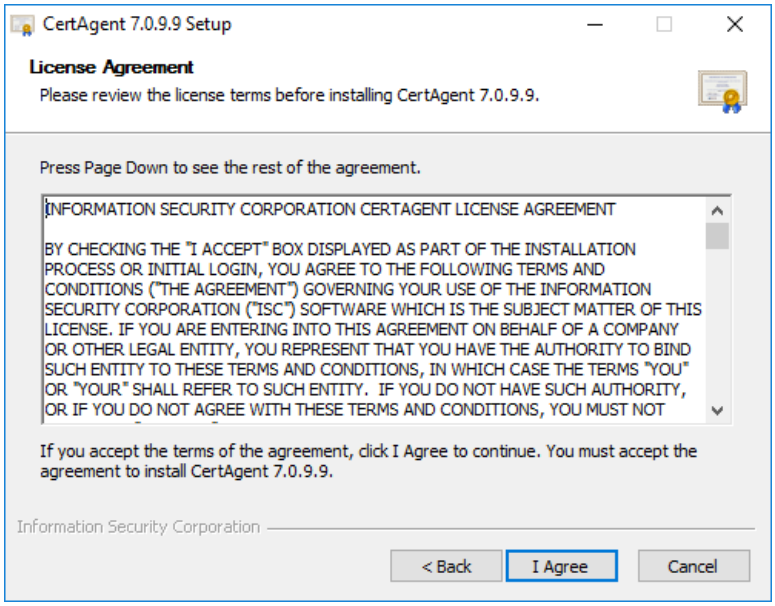
3.2.1 Windows

CertAgent for Windows is packaged as a zip archive that may be unzipped into any convenient directory on your webserver's hard drive. After unzipping the archive, run `certagent.<version>.x64.exe` to install CertAgent. Once the installation program begins, just follow the on-screen instructions.

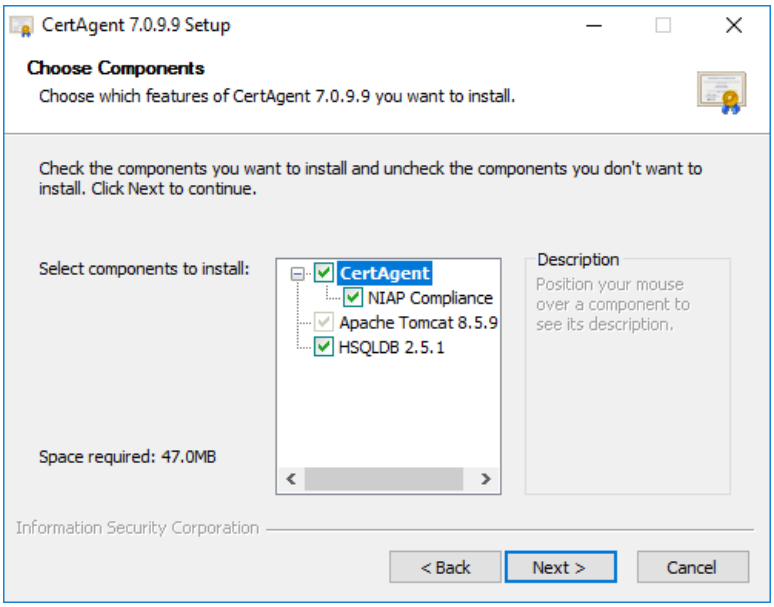
1. The installation program begins:



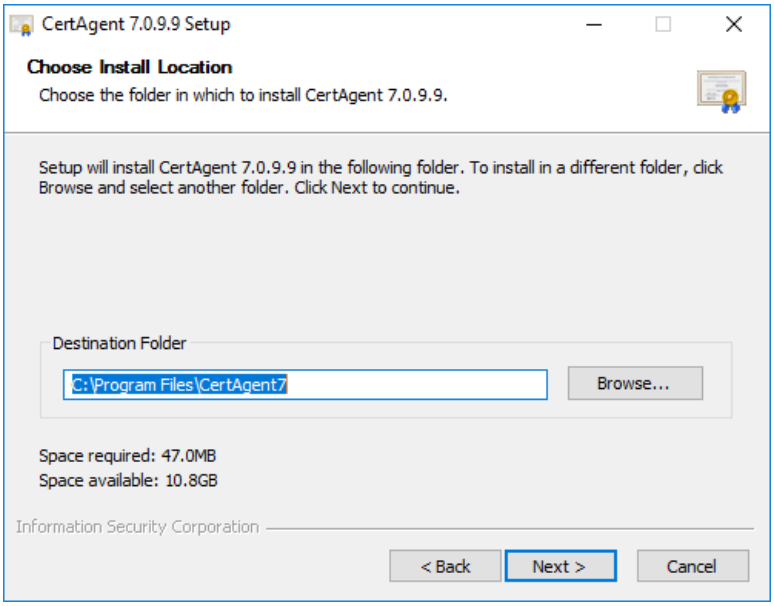
2. Click **Next**. The License Agreement page will appear:



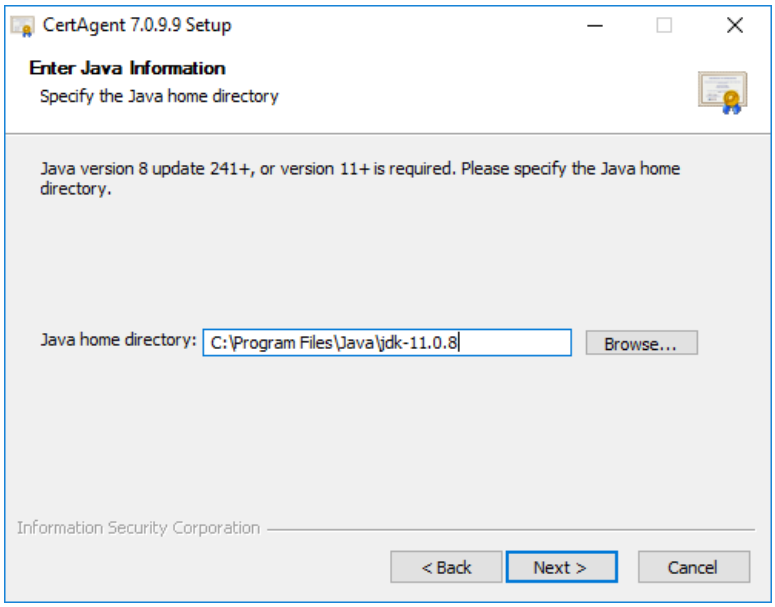
3. Review the agreement and click **I Agree**. The Choose Components page will appear:



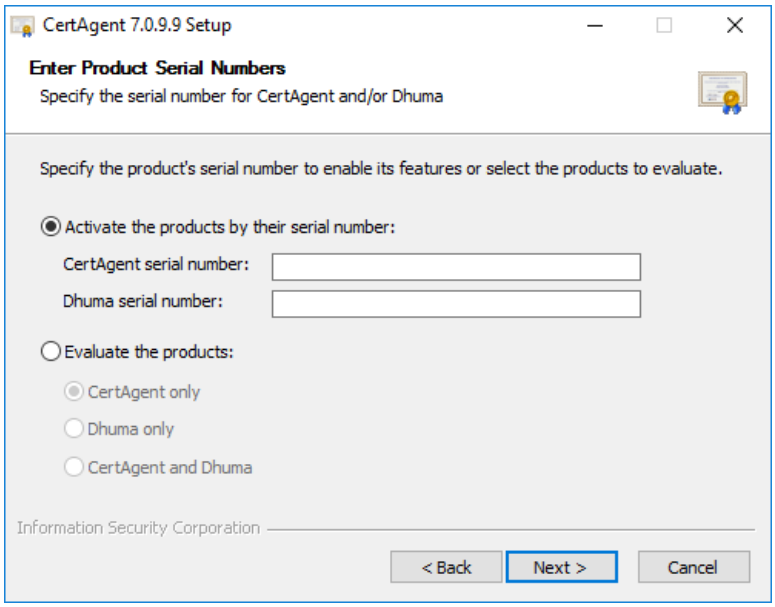
4. Keep all the components checked. NIAP compliance TOE and HyperSQL database will be installed. Click **Next**. The Choose Install Location page will appear:



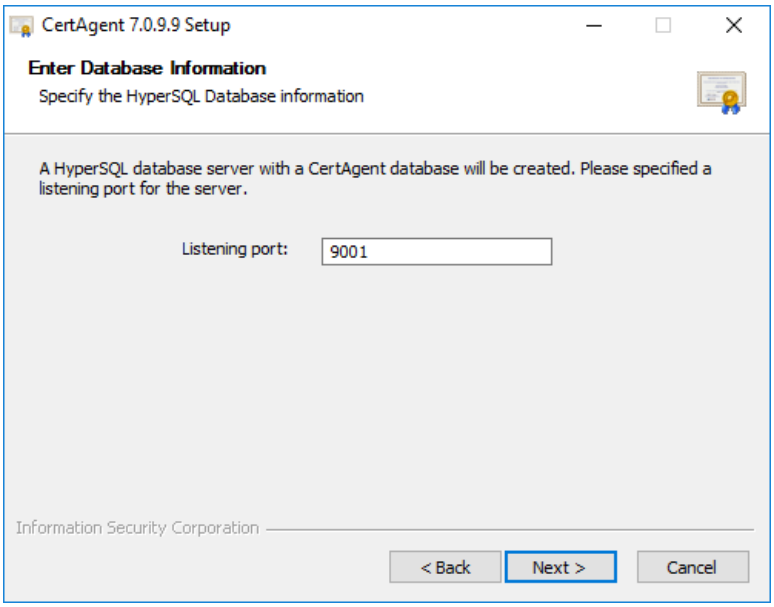
5. Change the destination folder if needed. Then, click **Next**.



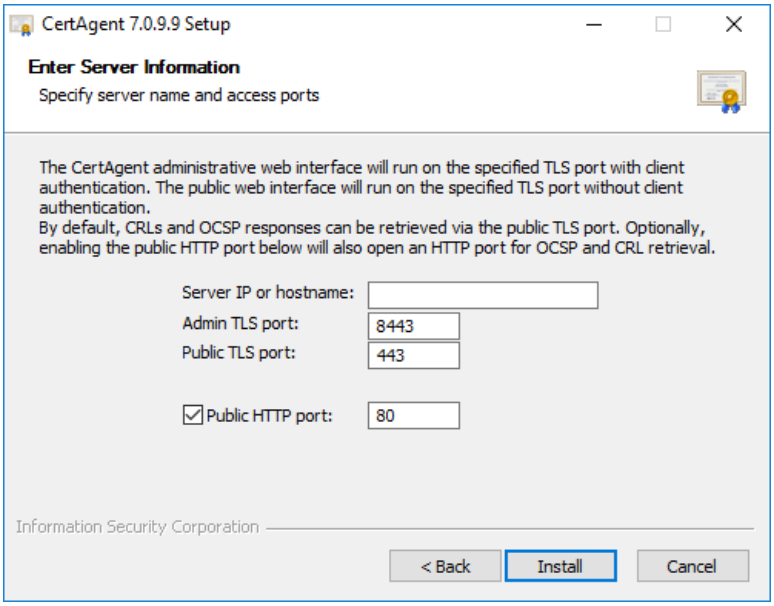
6. Click **Browse…** and select the Java 11.0.8 home directory. Then, click **Next**.



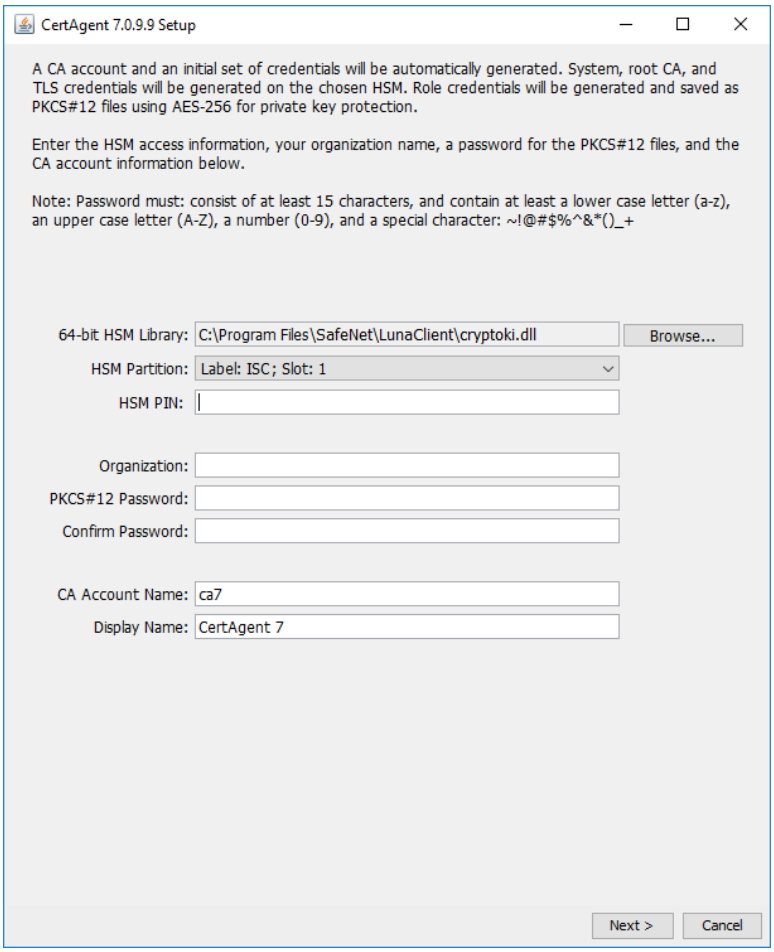
7. Enter CertAgent and Dhuma serial numbers to activate the products and enable enhanced OCSP support. Then, click **Next**.



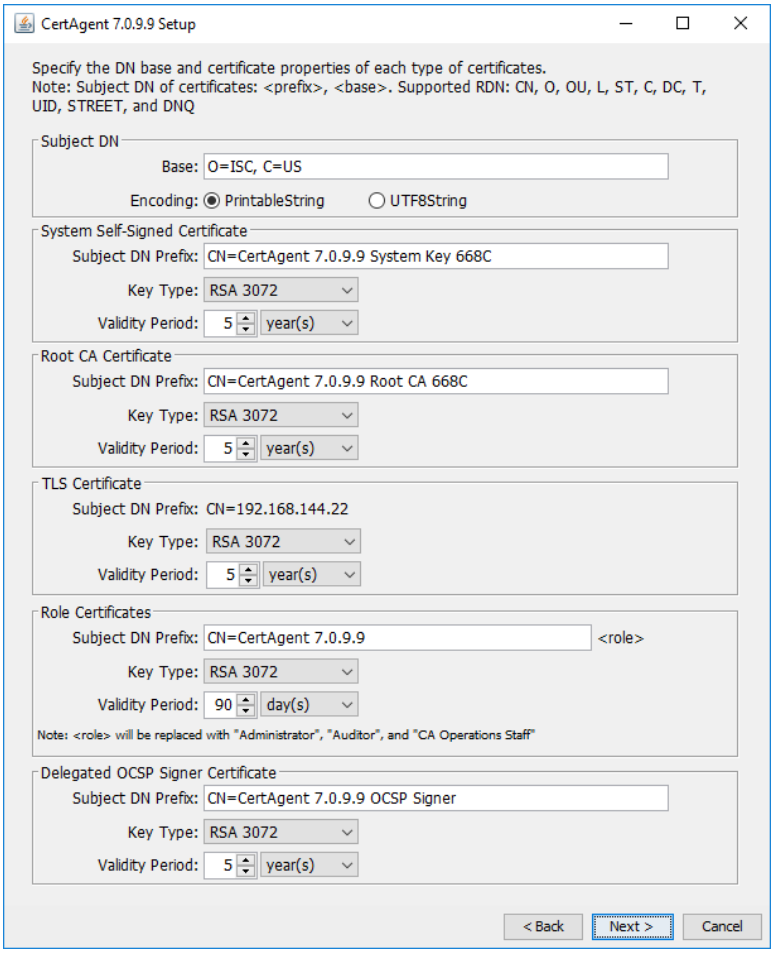
8. Change the port if needed. Then, click **Next**.



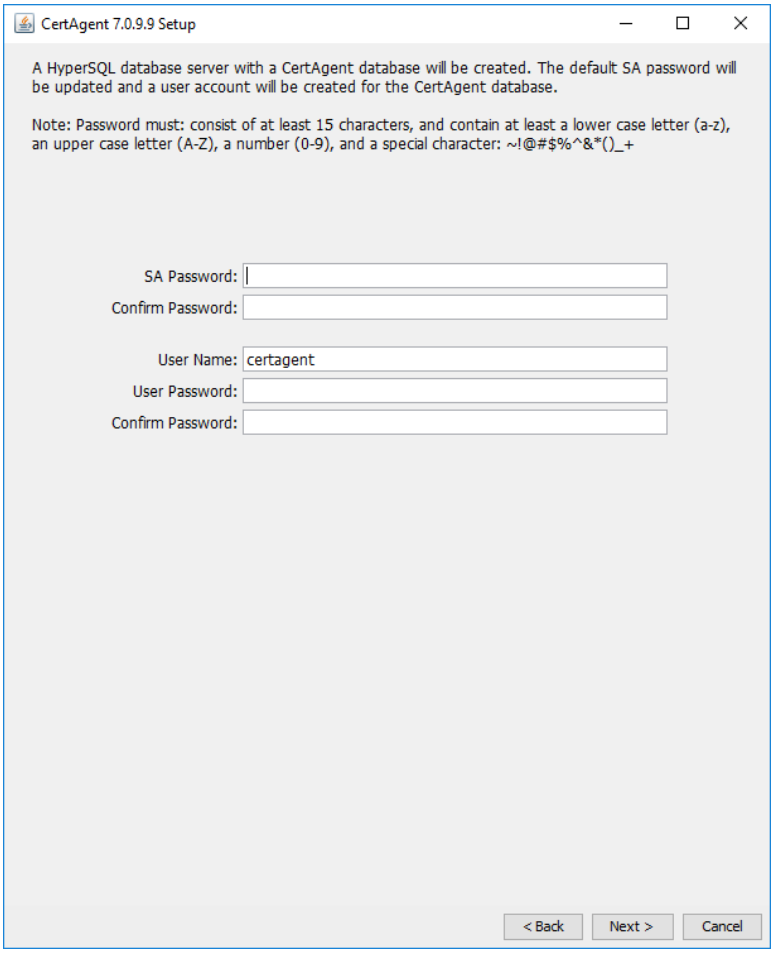
9. Enter the server IP address or hostname of the system. Change the ports if needed. Then, click **Install**. The installation of program files will begin. The following CertAgent Setup dialog will appear:



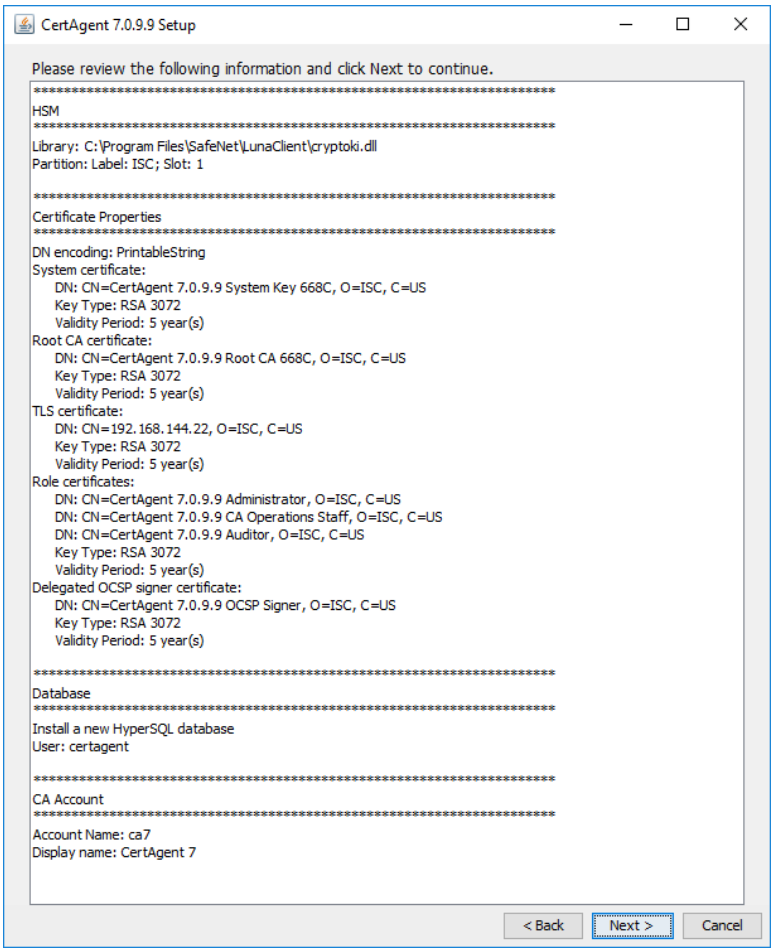
10. Click **Browse…** to select the 64-bit HSM library: `C:\Program Files\SafeNet\LunaClient\cryptoki.dll`. The HSM partition drop-down will be populated automatically. Select the desired partition and enter the HSM PIN. Complete the rest of the form and click Next.



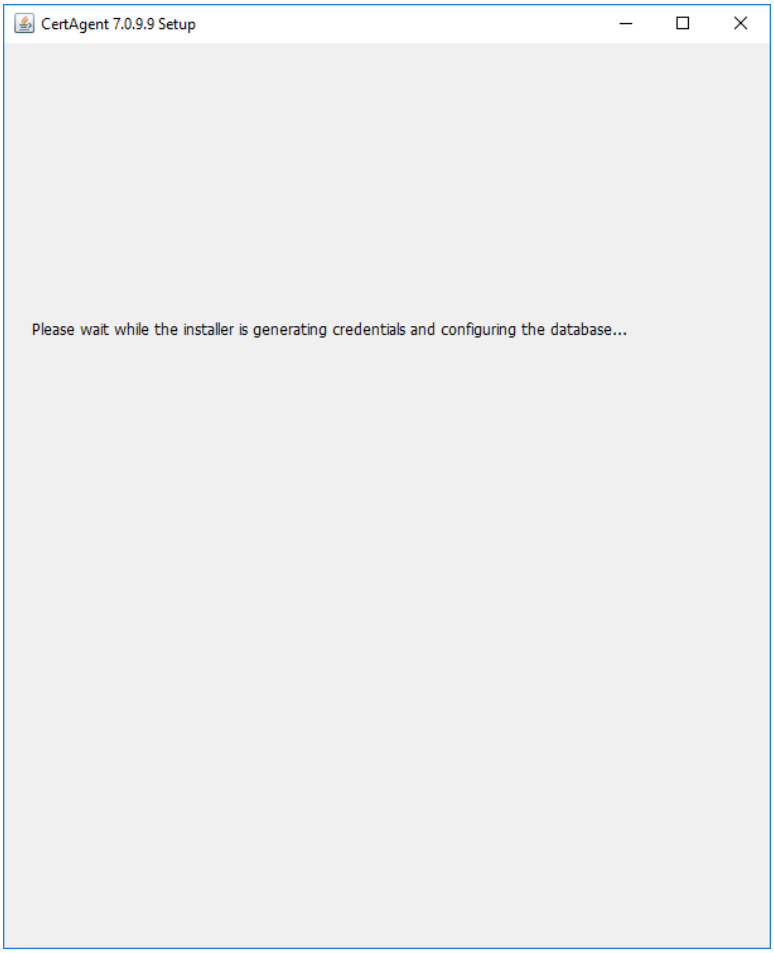
11. Change the certificate properties if needed. Then, click **Next**.



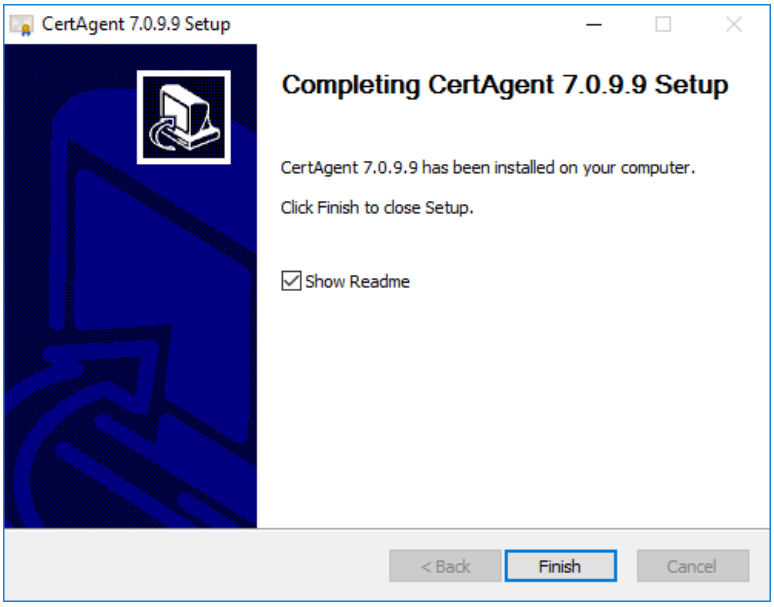
12. Enter the passwords and click **Next**.



13. Review the information and click **Next.** Key generations will begin:



14. Once it is done, the Finish page will appear:



15. Click **Finish.** The Readme file will appear. The details of the installation are saved to `<ca home>\install.log`.

3.2.2 CentOS

Before installing CertAgent, make sure the PostgreSQL JDBC driver has already been installed in the Operating System, and the directory containing the 64-bit HSM library is included in the LD_LIBRARY_PATH.

Login to the CentOS as root and run the following commands to include the HSM library directory (`/usr/safenet/lunaclient/lib`) in the LD_LIBRARY_PATH:

```
LD_LIBRARY_PATH=/usr/safenet/lunaclient/lib
export LD_LIBRARY_PATH
```

The CertAgent package for CentOS platforms consists of a tar archive that may be unzipped (with directory structure preserved) into any convenient directory on your webserver's hard drive.

To install CertAgent:

1. Run the following commands to unpack the archive and run the installation script:

   ```
   tar –xzf certagent.<version>.lnx.x64.tar.gz
   cd certagent.<version>-install
   ./install.sh
   ```

2. The installation program begins. Press ENTER to confirm the LD_LIBRARY_PATH.
3. A license agreement will then be displayed. Enter 'yes' to accept the license agreement.
4. In the installation type section, enter '1' to select NIAP-compliance option.
5. In the installation directory section, press ENTER to accept the default installation directory (/usr/local/certagent7).
6. In the Java installation directory section, press ENTER to accept the default Java directory or enter the Oracle Java 11.0.8 installation directory.
7. In the product(s) section, enter '3' to install both CertAgent and Dhuma. Then enter '1' to activate the selected products.
8. In the serial number section, enter the CertAgent and Dhuma serial numbers.
9. In the host name or IP address section, press ENTER to accept the specified host name or enter the IP address of your system.
10. In the ports section, press ENTER to accept the public HTTPS access (default to 443) and admin HTTPS access (default to 8443) ports. Press ENTER to open an HTTP port for OCSP and CRL retrieval. Press ENTER to accept the HTTP port (default to 80).

11. In the database section, enter ‘2’ to use an existing PostgreSQL database. Enter the location of the PostgreSQL’s JDBC driver (postgresql-42.2.16.jar).
12. In the confirmation section, press ENTER to confirm the configuration. Program files will then be extracted.
13. In the HSM info section:
    a. Press ENTER to accept the Luna library location (`/usr/safenet/lunaclient/lib/libCryptoki2_64.so`).
    b. Available partitions for the specified HSM library will be displayed. If there is only one partition found, press ENTER to select this partition. Otherwise, enter the ID of the desired partition.
    c. Enter the HSM PIN.
14. In the subject DN base and encoding screen:
    a. Enter the DN base (e.g., O=ISC, C=US). This base will be used to populate the subject DN of the initial certificates.
    b. Press ENTER to accept the DN encoding (default to PrintableString).
15. In the system self-signed certificate properties screen:
    a. Press ENTER to accept the DN prefix (default to CN=CertAgent <version> System Key <4 random characters>).
    b. Press ENTER to accept the key type (default to RSA 3072).
    c. Press ENTER to accept the validity period (default to 5 years).
16. In the Root CA certificate properties screen:
    a. Press ENTER to accept the DN prefix (default to CN=CertAgent <version> Root CA <4 random characters>).
    b. Press ENTER to accept the key type (default to RSA 3072).
    c. Press ENTER to accept the validity period (default to 5 years).
17. In the TLS certificate properties screen:
    a. Press ENTER to accept the key type (default to RSA 3072).
    b. Press ENTER to accept the validity period (default to 5 years).
18. In the role certificate properties screen:
    a. Press ENTER to accept the DN prefix (default to CN=CertAgent <version>).
    b. Press ENTER to accept the key type (default to RSA 3072).
    c. Press ENTER to accept the validity period (default to 90 days).
19. In the Delegated OCSP Signer certificate properties screen:
    a. Press ENTER to accept the DN prefix (default to CN=CertAgent <version> OCSP Signer).
    b. Press ENTER to accept the key type (default to RSA 3072).
    c. Press ENTER to accept the validity period (default to 5 years).
20. In the private key and keystore password section, enter a new password. Enter the same password again to confirm.

21. In the confirmation section, view the information and press ENTER to continue.
22. In the CA account name screen:
    a. Press ENTER to accept the CA name (default to ca7).
    b. Press ENTER to accept the CA display name (default to CertAgent 7).
23. In the database configuration screen:
    a. Enter the database access URL:
    `jdbc:postgresql://<host>:<port>/<database>`.
    b. Enter the database user name.
    c. Enter the password of the specified user name.
24. The installer will then generate the System, Root CA, TLS, and authentication credentials, configure CertAgent and start CertAgent service. The result will be displayed on the screen.

4. Managing the TOE

4.1 Starting and Stopping the Service

By default, the TOE service starts and stops automatically upon system start-up and shut-down. The Tomcat service starts automatically upon system PIN entry and stops upon TOE shut-down. If the HyperSQL database server was installed as part of the CertAgent package, its service starts and stops automatically as well.

4.1.1 Managing the TOE Service

To manage the TOE Service:

An OE Administrator must log into the environmental Operating System.

On CentOS, run the following commands to start or stop the CertAgent service manually:

```
sudo systemctl [start|stop] isc-certagent7
```

You can check the status of CertAgent service by running the following commands:

```
sudo systemctl status isc-certagent7
```

On Windows, open the Services program, select “CertAgent Server Controller”, click the start or stop button to start or stop the CertAgent and HyperSQL database services manually.

You can check the status of the CertAgent service by running the following commands:

```
C:\Program Files\CertAgent7\certagent.bat status
```

4.1.2 Starting the Service in Maintenance Mode

When a fatal error occurred (e.g., failure of integrity is detected), CertAgent will display an error message and shut itself down in an orderly manner. An OE Administrator must start CertAgent in maintenance mode by logging into the environmental Operating System and run the following commands:

```
sudo <ca home>/certagent.sh start-maintenance                    (CentOS)
<ca home>\certagent.bat start-maintenance                       (Windows)
```

When CertAgent is running in a maintenance mode, only the Admin Site will be accessible by authorized users, and the following NIAP conformance options will be disabled:

- Enable data integrity on the Trust Anchor list
- Enable data integrity on ACLs
- Run integrity tests on server startup

- Enable strict certificate and path validations
- Enable restrictions on security roles

An administrator should login to the Admin Site to resolve the issue. Once the issue has been fixed, an administrator should enable all the NIAP conformance options and log out. An OE administrator should stop the CertAgent service manually by running the commands:

```
sudo <ca home>/certagent.sh stop                    (CentOS)
<ca home>\certagent.bat stop                        (Windows)
```

On Windows, open Services program, select "CertAgent Server Controller", click the restart button. On CentOS, run the following command:

```
sudo systemctl start isc-certagent7
```

4.2 Entering System PIN

Sensitive data is encrypted with the system certificate and stored in the database and configuration file. An OE Administrator must enter the PIN of the HSM in which the system credential resided on each time the system is booted via the CertAgent script.

To enter the system PIN, run the following command:

```
sudo <ca home>/certagent.sh setpin                  (CentOS)
<ca home>\certagent.bat setpin                      (Windows)
```

4.3 Importing Privileged User Credentials into Firefox

CertAgent's web-based administrative interface may be accessed by authorized users.

An initial (temporary) set of role certificates (`<ca home>/keystore/ca-admin.der`, `ca-operations-staff.der`, and `ca-auditor.der`) is automatically added to the ACL during installation. You should import these temporary credentials (`<ca home>/keystore/ca-admin.p12`, `ca-operations-staff.p12`, and `ca-auditor.p12` with password `<p12 pass>`) into your web browser's certificate store in order to gain access to the CertAgent site.

AES-256 is used to encrypt your private key during the installation. The PKCS#12 files generated by the installer can only be imported to compatible browsers (e.g., Firefox 56+).

To import the administrator's credentials into Firefox:

1. Select the **Menu** button and select **Preferences** on UNIX or **Options** on Windows.
2. From the left-side menu, select **Privacy & Security**.
3. Click **View Certificates**.

4. In the Certificate Manager dialog, select the 'Your Certificates' tab and click **Import**.

5. Browse to the PKCS#12 file (e.g., `<ca home>/keystore/ca-admin.p12`) and click **Open**.

6. Enter the password that was used to encrypt the private key and click **OK**.

7. Firefox will alert you when the certificate has been installed successfully.

8. Select the 'Authorities' tab, select the root certificate (e.g., `CertAgent <version> Root CA XXXX`) listed under the organization you have entered during the installation.

9. Click **Edit Trust**, click both checkboxes in the Edit CA certificate trust settings dialog and click **OK**.

4.4 Managing the Administrative Site

4.4.1 Logging in the Administrative Site

To access the CertAgent system administration login page, launch Firefox and enter the following URL into its address bar:

```
https://<hostname/IP address>:<admin port>/certagentadmin/admin/login.jsp
```

Be sure to replace `<hostname/IP address>` and `<admin port>` with the appropriate system name or IP address and TLS port of your CertAgent webserver. Select your role certificate (*e.g.,* CertAgent *<version>* Administrator) in the security dialog to authenticate yourself to the webserver, and then click **OK**.

A page with an access banner and a Login button will appear. Click **Login**. The status page will appear with a welcome message: "Welcome! You are currently logged in as the site <administrator or auditor> (<subject DN of the client certificate>)."

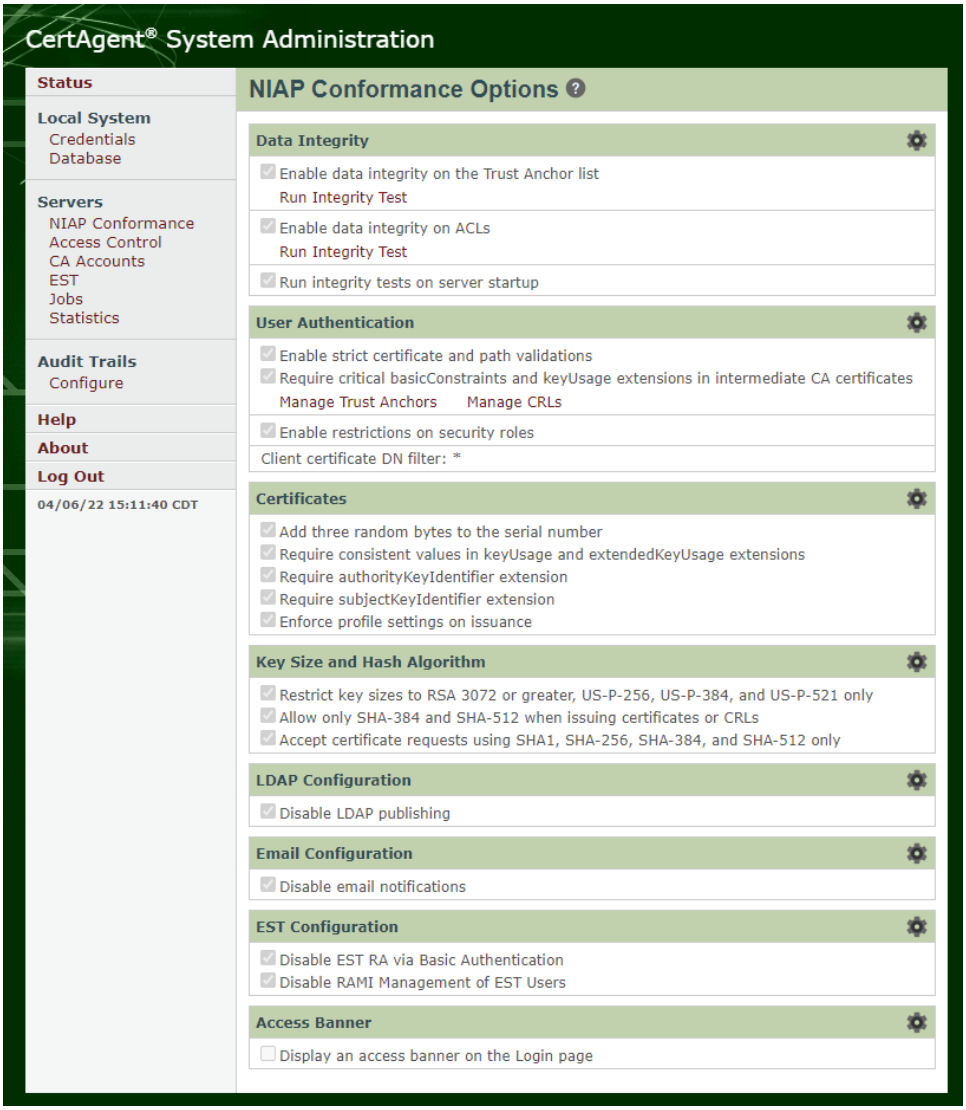
For more information on server management and how to use the administrative site, please refer to the online help system:

```
https://<hostname/IP address>:<admin port>/certagentadmin/admin/help.html
```

4.4.2 Managing NIAP Conformance Settings

To manage NIAP conformance settings:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Servers, NIAP Conformance**. The following page will appear:



NOTE: In order for the TOE to operate in NIAP compliant mode, all settings in this page must be checked. The following sections describe each option in detail.

4.4.2.1 Data Integrity

The integrity of the trust anchor table, and the table storing the ACLs, is maintained using a digital signature created using the CA "System" credential. This signature is validated when the table is used. The signature is updated whenever an administrator modifies the trust list or ACLs. Integrity can optionally be verified at power-up (after the system PIN has been entered to enable access to the database) and on-demand by an Admin Site Administrator.

In case of any integrity failure occurring, CertAgent will record the error in both the audit trail and local server log file, destroy any sensitive data, and shut down the CertAgent service. A local administrator must restart CertAgent in maintenance mode, which will disable the integrity test, path

validation, and security role restriction. They will then need to remove all certificates from the corresponded list and reimport the certificates to the list via the web interface or CACLI.

4.4.2.1.1 Updating the Settings

To update the settings:

1. Click the  icon in the Data Integrity section.
2. Update the settings as desired and click **Update**.

   Available options are:
   - Enable database integrity on the Trust Anchor database
   - Enable database integrity on the ACL database
   - Run integrity tests on server startup

   The result will be displayed.

NOTE: If an integrity setting is changed from disabled to enabled, a signature of the associated table will be created automatically. You will be prompted to confirm your intention. Click **OK** to continue.

4.4.2.1.2 Running Integrity Test on Demand

To run the integrity test on demand:

1. Click the **Run Integrity Test** link of the desired list.
2. Click **OK** at the confirmation prompt to confirm your intentions.
   The result will be displayed.

4.4.2.2 User Authentication

4.4.2.2.1 Certificate and Path Validations

Certificates used to authenticate to the CertAgent web interfaces are validated first by Apache Tomcat:

- Certificate validation and certificate path validation
- The certificate path must terminate with a certificate in the Trust Anchor keystore configured in the servlet container

If the certificate and path validations option is enabled, the certificate will be validated again by CertAgent:

- IETF RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a certificate in the Trust Anchor Database managed by the CertAgent Administrator

- CertAgent requires that intermediate and root certificates contain a basicConstraints extension asserting the CA flag
- CertAgent checks the revocation status of the user and intermediate certificates using Certificate Revocation Lists (CRLs) managed by the CertAgent Administrator
- The end entity certificate presented must have the Client Authentication usage (OID 1.3.6.1.5.5.7.3.2) set in the extendedKeyUsage field
- If the Require critical basicConstraints and keyUsage extensions in intermediate CA certificates option is enabled, CertAgent requires all intermediate certificates in the certification path critical basicContraints and keyUsage extensions

To manage the Trust Anchor database:

1. Click the **Manage Trust Anchors** link in the User Authentication section.
2. To add a trust anchor certificate to the list, click **Add**, then upload it by clicking **Browse…**, locating the appropriate certificate file (X.509 certificate or PKCS#7), and clicking **Upload**. A confirmation message will be displayed.

   NOTE: Only valid self-signed certificates containing a basicConstraints extension asserting the CA flag can be imported into the list.
3. To inspect a particular certificate, click on its DN. A popup dialog with certificate information will appear. Click **Close** to close the dialog.
4. To remove one or more certificates from the list, check the boxes of those you wish to delete and click **Remove**. Then click **OK** in the confirmation dialog.

To manage the CRLs used for path validation:

1. Click the **Manage CRLs** link in the User Authentication section.
2. To add a CRL to the list, click **Add**.
3. If the CRL you wish to install is issued by a CA account on the same system, select 'Retrieve CRL automatically from CA account automatically'. Select the desired CA account from the drop-down. The CRL will update automatically when it is issued. In addition to the CRL check during the path validation, the status of the user certificate will be checked from the issuer account. If the certificate has been revoked but not yet included in a CRL, the path validation will fail.

   To manage the CRL manually, select the 'Upload a CRL' option and click **Browse…** to locate the appropriate CRL file.
4. Click Add. A confirmation message will be displayed.
5. To inspect a particular CRL, click on its DN. A popup dialog with certificate information will appear. Click **Close** to close the dialog.

   To remove one or more CRLs from the list, check the boxes of those you wish to delete and click **Remove**. Then click **OK** in the confirmation dialog.

4.4.2.2.2 Restrictions on Security Roles

CertAgent supports three roles (Administrator, Auditor, and CA Operations Staff), each of which consists of an access control list (ACL) of one or more X.509 certificates and one or more rights (admin, audit, certify, revoke, RAMI, and DBAccess).

If restrictions on security roles are enabled, CertAgent refuses to allow the same certificate to be placed:

- on both an Audit ACL and a non-audit ACL in the Admin Site
- on both an Audit ACL and a non-audit ACL within a given account on the CA Site
- on both a CA Operations Staff ACL and a non-CA Operations Staff ACL for a given account on the CA Site

In order to operate CertAgent properly, at least three different credentials are required. Each certificate needs to be uploaded to the appropriate ACL with 'admin', 'audit', or 'CA operations staff' permissions.

4.4.2.2.3 Client Certificate DN Filter

CertAgent supports filtering client certificates by their distinguished name (DN) in order to allow an administrator to restrict access to only matching certificates. If a client certificate's DN does not match the configured filter, the TOE responds with a fatal TLS 'bad_certificate' error.

By default, the filter is set to '*' to allow any DNs. Specify a DN filter with RDN components, and one or more asterisk as appropriate to the DN structure of your role certificates. For example: CN=*, O=ISC, C=US.

4.4.2.2.4 Updating the Settings

To update the settings:

1. Click the  icon in the User Authentication section.
2. Check or uncheck **Enable certificate and path validations**, **Require critical basicConstraints and keyUsage extensions in intermediate CA certificates** and **Enable restrictions on security roles** checkboxes, or update the **certificate DN filter** as desired and click **Update**.

4.4.2.3 Certificates

4.4.2.3.1 Adding Random Bytes to the Serial Number

CertAgent uses the database sequence to keep track of the next sequential number. If this option is enabled, each 20 byte serial number consists of 3 leading random bytes and 17 bytes representing the next sequential number, padded with leading zeros. The random bytes are obtained from the ISC CDK.

4.4.2.3.2 Requiring Consistent Values in keyUsage and extendedKeyUsage Extensions

If this option is enabled, the following purposes in the extended key usage extension must be set with the specified purpose in the key usage extension:

- Server authentication (1.3.6.1.5.5.7.3.1) must be set with digital signature, key encipherment or key agreement
- Client Authentication (1.3.6.1.5.5.7.3.2) must be set with digital signature and/or key agreement
- Code signing (1.3.6.1.5.5.7.3.3) must be set with digital signature
- Email protection (1.3.6.1.5.5.7.3.4) must be set with digital signature, non-repudiation, and/or (key encipherment or key agreement)
- Time stamping (1.3.6.1.5.5.7.3.8) must be set with digital signature and/or non-repudiation
- OCSP signing (1.3.6.1.5.5.7.3.9) must be set with digital signature and/or non-repudiation

4.4.2.3.3 Requiring Authority Key Identifier Extension

If this option is enabled, any certificates issued by a CA account must have the authority key identifier extension.

4.4.2.3.4 Requiring Subject Key Identifier Extension

If this option is enabled, any certificates issued by a CA account must have the subject key identifier extension.

4.4.2.3.5 Enforcing Profile Settings on Issuance

If this option is enabled, any certificates issued by a CA account must use the profile settings.

4.4.2.3.6 Updating the Settings

To update the settings:

1. Click the  icon in the Certificates section.
2. Update the settings as desired and click **Update**.

4.4.2.4 Key Size and Hash Algorithm

4.4.2.4.1 Restricting Key Sizes to RSA 3072 or Greater, US-P-256, US-P-284, and US-P-521 only

If this option is checked, only RSA 3072 or greater, US-P-256, US-P-284, and US-P-521 key pairs can be generated, and certificate requests will be accepted.

4.4.2.4.2 Allowing only SHA-384 and SHA-512 When Issuing Certificates and CRLs

If this option is checked, only SHA-384 and SHA-512 are allowed when issuing certificates and CRLs.

4.4.2.4.3 Accepting Certificate Requests using SHA1, SHA-256, SHA-384, and SHA-512 only

If this option is checked, only certificate requests using SHA1, SHA-256, SHA-384, and SHA-512 will be accepted.

4.4.2.4.4 Updating the Settings

To update the settings:

1. Click the  icon in the Key Size and Hash Algorithm section.
2. Update the settings as desired and click **Update**.

4.4.2.5 LDAP Configuration

If 'Disabling LDAP Publishing' option is checked, LDAP publishing will be disabled.

4.4.2.6 Email Configuration

If 'Disabling Email Notification' option is checked, email notifications will be disabled.

4.4.2.7 EST Configuration

4.4.2.7.1 Disabling EST RA via Basic Authentication

If this option is checked, only EST users with one-time password can be created in the Self-Service page of the CA Account site and enroll using EST via basic authentication. The EST RA option will not be available.

4.4.2.7.2 Disabling RAMI Management of EST Users

If this option is checked, EST users can only be managed via the CA account site. The “Allow EST user management” option will not be available in the RAMI page of the CA Account site.

4.4.2.7.3 Updating the Settings

To update the settings:

1. Click the  icon in the EST Configuration section.
2. Update the settings as desired and click **Update.**

4.4.2.8 Access Banner

Before establishing a login session to the CertAgent, a configurable advisory notice and consent warning banner can be displayed on the Login pages of the Admin and CA account sites.

To manage the access banner:

1. Click the  icon in the Access Banner section.
2. To add an access banner, check the **Display an access banner on the Login page** checkbox. Enter the warning messages (plain text and HTML are allowed) in the text area and click **Update**.
3. To remove the access banner, uncheck the **Display an access banner on the Login page** checkbox and click **Update**.

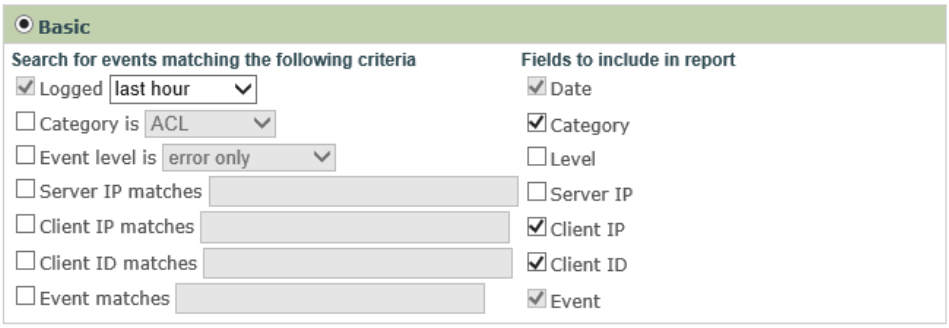
To view the access banner in Admin site, follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your role certificate.

To view the access banner in CA account site, follow the steps in Section *4.5.1 Logging in the CA Account Site* and select your role certificate.

4.4.3 Searching the Audit Trail

To search the audit trail of Admin Site:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your auditor certificate with 'audit' permission.
2. In the left panel, click **Audit Trails, Search.**
3. To search the audit trails using the basic search criteria:



Specify the desired search criteria and the fields to be included in the report. You may use an asterisk (*) as a wildcard in the search string.

The descriptions of each setting on this page are given in the following table:

Settings	Description
Date	Timestamp of the event in string Available options: last hour, last 12 hours, today, last 7 days, last 30 days, and custom
Category	Type of the event: credential, PIN, ACL, audit, login, database, job, CA account, email, NIAP, DBAccess, system, and TLS session; If not specified, all types will be displayed
Event level	Level of the event: INFO or ERROR. If specified, either error only and information only can be set. If not specified, both information and

	error events will be displayed.
Server IP	IP address of the CertAgent system
Client IP	IP address of the client system To search for events triggered by the system, enter [system]. To search for events triggered by the CACLI, installer, startup script, and update tool, enter CACLI, Installer, Startup Script, and Update Tool respectively.
Client ID	The identity of the client in string: Subject DN of an authorized user's certificate, CACLI, Installer, Startup Script, or Update Tool
Event	Recorded events

TABLE 11 AUDIT TRAIL SETTINGS

4. To search the audit trails using a SQL statement:
   a. Select the 'Advanced' option.
   b. Specify one or more columns to be included in the first text area and optionally specify the WHERE clause in the second text area to construct the desired SQL statement.

      To search for events triggered by the system, use "CLIENT IS NULL" in the WHERE clause.
      To search for events triggered by the CACLI tool, use "CLIENT='CACLI'" in the WHERE clause.
5. Click **Search** to search for the events. Result will be displayed in the **Result** tab.
6. To export the list of displayed events to a file in CSV format, click **Export Search Result to File**.
7. To save the search to reuse, click **Save Search**.
   a. Select **Save** to overwrite the existing search.
   b. Otherwise, select **Save as** and specify a name.
8. Click **Save** to apply the changes.

4.4.4 Configuring Audit Trail Settings

To configure the audit trail setting:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your admin certificate with 'admin' permission.
2. In the left panel, click **Audit Trails, Configure.**
3. To configure the audit trail of the Admin Site setting:
   a. Click the  icon in the CertAgent Admin Site section.
   b. Check or uncheck the desired options.

c. Click **Update**.

4.4.5 Creating a New CA Account

To create a new CA Account:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Servers, CA Accounts.**

   Then complete the new account form.
   The descriptions of each setting on this page are given in the following table:

Setting	Description
Account Name	A unique identifier for a Certificate Authority; may only contain the characters A-Z, a-z, and 0-9. This name will be embedded in the system URIs for certificates and CRL retrieval.
Display Name	The friendly name of the account; may only contain the characters A-Z, a-z, 0-9, and space.
CA Description	The description of this CA as it will appear on the CA Resources page of the public site

TABLE 12 CA ACCOUNT SETTINGS

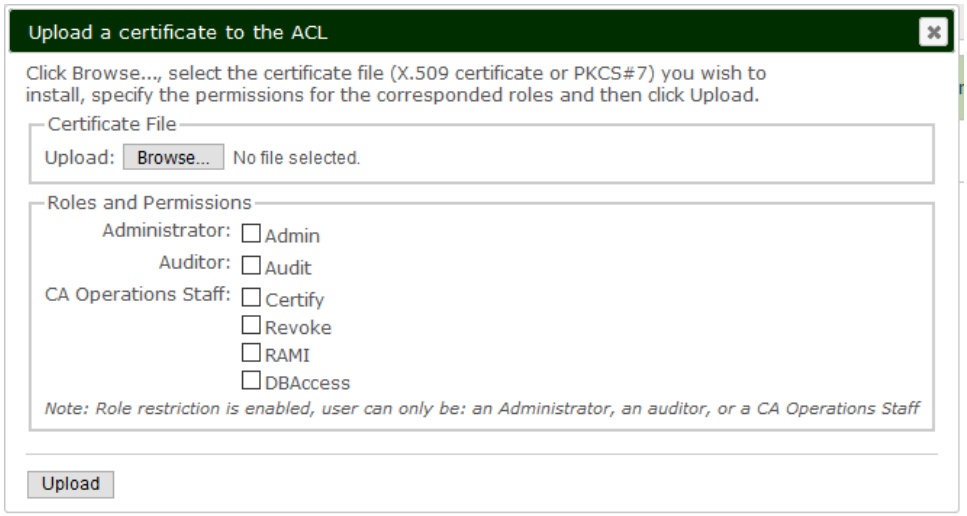
3. Click **Create**.
   A new CA account will be created and a confirmation message will be displayed.

4.4.6 Managing an Existing CA Account

4.4.6.1 Managing the ACL

To view or modify the ACL for an existing account:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Servers, CA Accounts.**
3. Click the  icon for the CA account you wish to modify.
4. Click **Add**. The following form appears:



5. Upload a certificate by clicking **Browse…**, locating the appropriate certificate file, selecting the desired role and its permissions:

   - Administrator with 'admin' permission
   - Auditor with 'audit' permission
   - CA Operations Staff with 'certify', 'revoke', 'RAMI', and/or 'DBAccess'.

   The following table describes the administrative permissions available for a CA account and the corresponding responsibilities:

Role	Permission	Responsibility
Administrator	admin	manage account configurations (issuer credential, certificate profile, CRL issuance, certificate issuance, EST, OCSP, and enrollment options)
Auditor	audit	view and export audit trails, and search certificates
CA Operations Staff	certify	issue certificates, reject invalid certificate requests, manage EST subscribers, manage automated certificate issuance option, and manage RAMI enrollment setting
	revoke	revoke certificates, issue CRLs, manage self-service certificate revocation option, manage automated CRL issuance option, manage RAMI CRL issuance, and revocation settings
	RAMI	submit requests via the RA management interface (RAMI)
	DBAccess	submit queries via the DBAccess service

TABLE 13 CA ACCOUNT ROLES AND PERMISSIONS

6. Click **Upload**. A confirmation message will be displayed.

   NOTE: Only end-user certificates in a PKCS#7 file will be installed; any CA certificates in the file are ignored.

   NOTE: A user certificate can be assigned to one role (Administrator, Auditor, or CA Operations Staff). If CA Operations Staff is selected, one or more permissions (Certify, Revoke, RAMI, and DBAccess) can be assigned.

7. To update the permission of an existing user, click the  icon for the certificate you wish to modify. Uncheck the current permissions, check the desired permissions, and click **Update**.
8. To inspect a certificate, click on the desired certificate DN. A popup dialog with certificate information will be displayed. Click **Close** to close the dialog.
9. To remove one or more certificates from the ACL, check the boxes of those you wish to delete and click **Remove**. Then click **Yes** in the confirmation dialog.

4.4.6.2 Disabling a CA Account

When a CA account is no longer in service, it can be disabled. Once disabled, the ACL of the CA account will be deleted, and this account will not be accessible from any interface. However, the requests, certificates, CRLs, account configuration, and audit trails will remain in the database.

To disable one or more CA Accounts:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Servers, CA Accounts.**
3. Check one or more CA accounts you wish to disable.
4. Click **Disable** and **OK** to confirm the operation.

To enable one or more CA Accounts:

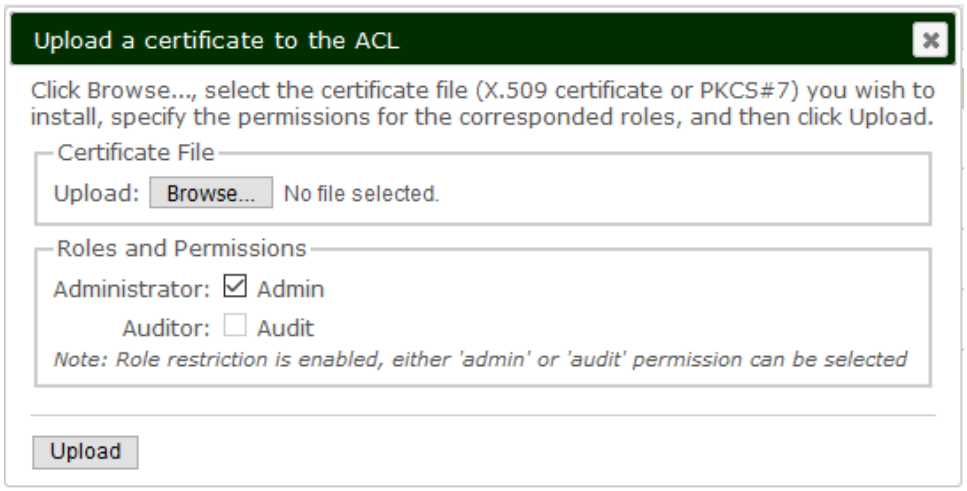
1. In the left panel, click **Servers, CA Accounts.**
2. Select the **Disabled** tab.
3. Check one or more CA accounts you wish to enable.
4. Click **Enable Acc**ount and **OK** to confirm the operation.

4.4.7 Managing the Server Administration Access Control List

Authorized administrators or auditors can manage NIAP conformance options, create CA accounts, manage jobs, configure email settings, and audit trails from any CertAgent systems.

To manage the Server Administration ACL:

1. Follow the steps in section *4.4.1 Logging in the Administrative Site* to login and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Servers, Access Control.**
3. Click **Servers, Access Control** to view a list of the entities currently authorized to access the administrative pages on the current host (and on any other CertAgent system in a high-availability cluster to which the current host may belong).
4. To add a certificate to the ACL, click **Add**. The following form appears:



5. Upload a certificate by clicking **Browse…**, locating the appropriate certificate file, selecting the desired permissions: Admin or Audit.
6. Click **Upload**. A confirmation message will be displayed.
7. To update the permission of an existing user, click the icon for the certificate you wish to modify. Uncheck the current permission, check the desired permission, and click **Update**.
8. To inspect a particular certificate, click on its DN. A popup dialog with certificate information will appear. Click **Close** to close the dialog.
9. To remove one or more certificates from the ACL, check the boxes of those you wish to delete and click **Remove**. Then click **OK** in the confirmation dialog.

4.4.8 Managing System Credential

CertAgent has a set of system credentials used to protect all CA HSM PINs and passwords used in the various configurations settings.

To view the system credentials, click the **Local System, Credentials** item in the left-hand action menu.

To update the system credentials:

1. Click **Update**.
2. Select **Use default** to use the existing HSM access settings. Otherwise, select **Use custom** and specify the required HSM access information. To view the slots and labels available on your HSM, enter the path of the vendor-provided access library and click **View Slots/Labels**.
3. To generate a new key pair:
4. Select **Generate a new key pair** and click **Next**.
   a. Enter the RDNs and change the key type and size, message digest and validity period, if needed.
   b. Click **Next** and then **OK** at the confirmation prompt to confirm your intentions.

5. To select an existing key pair:
    a. Select **Use an existing key pair** and click **Next** to see a list of all sign- and encrypt-capable credentials on the specified HSM.
    b. Select the system certificate you wish to use. (To view detailed information about any of the available certificates, click its DN.)
    c. Click **Next** and then **OK** at the confirmation prompt to confirm your intentions.

NOTE: Each cloned CertAgent system in a high-availability cluster must be configured to use the same system credentials. To change the system credentials in a cluster, an authorized administrator must successively log in to each of the clones in the cluster using their individual IP addresses and update their system credentials manually.

4.4.9 Managing Enrollment over Secure Transport (EST)

CertAgent supports the following EST operations, authentications, and URLs:

Operation	Authentication	URL Format
Distributions of CA certificates	None	https://<host>:<public port>/.well-known/est/<ca>/cacerts
Enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/<ca>/simpleenroll
	Basic	https://<host>:<public port>/.well-known/est/<ca>/simpleenroll
Re-enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/<ca>/simplereenroll
	Basic	https://<host>:<public port>/.well-known/est/<ca>/simplereenroll

TABLE 14 EST OPERATIONS, AUTHENTICATIONS, AND URL FORMATS WITH A CA SEGMENT

By default, the CA account or profile name (<ca>) is embedded in the EST URLs. If a default EST account is set, the following EST URLs without the additional segment to specify the CA account or profile name will be supported. The EST requests will be submitted to the default account automatically.

Operation	Authentication	URL Format
Distributions of CA certificates	None	https://<host>:<public port>/.well-known/est/cacerts
Enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/simpleenroll
	Basic	https://<host>:<public port>/.well-known/est/simpleenroll

Re-enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/simplereenroll
	Basic	https://<host>:<public port>/.well-known/est/simplereenroll

TABLE 15 EST OPERATIONS, AUTHENTICATIONS, AND URL FORMATS WITHOUT A CA SEGMENT

To set a default EST account:

1. Click the **Servers, EST** item in the left-hand action menu and click **Create**.
2. Click the  icon.
3. Select the desired account from the **Default EST account** drop-down.
4. Click **Update**.

4.4.10 Managing Dhuma Accounts

CertAgent's OCSP capability is divided into basic OCSP support and enhanced OCSP support (Dhuma). Basic OCSP support provides OCSP responses for issuers managed by the CertAgent instance. Dhuma provides OCSP responses and CRL distribution points for issuers not managed by the CertAgent instance.

OCSP requests must contain only one target certificate identifier with or with a nonce. Requests must be submitted via HTTPS or HTTP POST with `Content-Type` header set to `application/ocsp-request` to the following URL:

```
http[s]://<host>:<port>/certagent/dhuma/ocsp
```

The CRL of an issuer can be downloaded from the following URL:

```
http[s]://<host>:<port>/certagent/dhuma/crl/<account>.crl
```

To manage Dhuma accounts and their configuration, click the **Servers, Dhuma** item in the left-hand action menu.

By default, the CRL distribution point option is enabled. To manage this setting, click the  icon in the CRL Distribution. Select the desired setting and click **Update**.

4.4.10.1 Creating a New Dhuma Account

To create a new Dhuma account:

1. Click **Create**.

2. Specify an account name (a unique identifier; may only contain the characters A-Z, a-z and 0-9).
3. Click **Create**.

4.4.10.2 Configuring OCSP Response Signer

OCSP responses must either be signed by the CA that issued the certificate in the OCSP request or by a CA delegated OCSP signer. CA certificate is required to have a digital signature purpose asserted in the Key Usage extension. A delegated OCSP signer certificate must be issued by the CA that is identified in the OCSP request and have a digital signature purpose asserted in the Key Usage extension and OCSP signing purpose asserted in the Extended Key Usage extension.

4.4.10.2.1 Generating a New Delegated OCSP Signer Credential

To generate a new delegated signer credential:

1. Click the  icon of the desired account.
2. Click the  icon in the OCSP Signer section.
3. Select 'Generate a new credential'. Select 'Use default' to use the existing HSM access settings. Otherwise, select 'Use custom' and specify the required HSM access settings. To view the slots and labels available on your HSM, enter the path of the vendor-provided access library and click **View Slots/Label**. Then, click **Next**.
4. Specify the RDNs. If necessary, change the encoding of DN, key type, and message digest.
5. Click **Generate**. Then, click **OK** in the confirmation dialog.
   CertAgent will:
   - generate a new key pair of the type you specified,
   - create a certificate request containing the public key, and
   - store the HSM access information with the HSM PIN encrypted under the system certificate, and certificate request into the database
6. Your request will then be displayed in base64-encoded format. Save the certificate request to a file that you may manually submit to a certificate authority for processing. Once the certificate has been issued, obtain the certificate and its certificate chain in a PKCS#7 file.
7. Click the  icon of the OCSP Response Signer Certificate Request section.
8. Upload the PKCS#7 file and click **Update**.
   If the OCSP signer certificate is valid, CertAgent will install the signer certificate into the HSM, and assign the signer credential and the CA certificate to the account.

4.4.10.2.2 Using an Existing Signer Credential

If you would like to use an existing CA or delegated signer credential, follow the instructions below.

1. Click the  icon of the desired account.
2. Click the  icon in the OCSP Signer section.
3. Select 'Use existing credential'. Select 'Use default' to use the existing HSM access settings. Otherwise, select 'Use custom' and specify the required HSM access settings. To view the slots and labels available on your HSM, enter the path of the vendor-provided access library and click **View Slots/Label**. Then, click **Next**.
4. All available CA credentials (certificates with the cA bit asserted in its basicConstraints extension, and the digitalSignature purpose asserted in its keyUsage extension) and delegated signer credentials (certificates with the cA bit not asserted in its basicConstraints extension, the digitalSignature purpose asserted in its keyUsage extension, and the ocspSigning purpose asserted in its extendedKeyUsage extension) on the HSM will be listed.
5. Select the desired credential. If a delegated signer credential is selected, upload the CA certificate file. Click **Next,** then **OK** at the confirmation prompt to confirm your intentions. The signer credential and CA certificate will be assigned to the account.

4.4.10.2.3 Configuring CRLs

The latest CRL of the issuer is used to determine the status of the requested certificate in an OCSP request. CRLs can be uploaded manually by an administrator or retrieved automatically from a URL.

To configure the CRL retrieval method:

1. Click the  icon of the desired account.
2. Click the  icon in the CRL Retrieval section.
3. If CRLs will be retrieved from a URL, select the 'Pull from a URL (HTTP only)' option, and specify the URL starting with 'http://' and the frequency. Otherwise, select the 'Load from a file' option and a CRL.
4. Click **Update**.

4.4.10.2.4 Configuring OCSP Response Settings

1. Click the  icon of the desired account.
2. Click the  icon in the OCSP Response Configuration section.
3. The options you can control on this page are:

Response caching	If enabled, the OCSP response without a nonce will be cached and reused for the same request. This option applies if the request does not have a nonce or the 'Exclude a nonce in the response' option is enabled.

nextUpdate field	nextUpdate field in the OCSP response. Available options: • Same as CRL's nextUpdate • Specify a time period from thisUpdate field
nonce field	Nonce field in the OCSP response. Available options: • Include the same nonce if found in the request • Exclude a nonce in the response • Reject the request with a nonce
Hash algorithm	Hash algorithm to sign the OCSP response. Available options: • SHA-1 • SHA-256 • SHA-384 • SHA-512

4. Edit these settings as desired, then click **Update**.

4.4.10.3 Removing Dhuma Accounts

When a Dhuma account is no longer in service, it can be removed. Once removed, all the configurations (signer, CA, CRL, and response) will be deleted. However, the signer credential will remain in the HSM, and audit trails will remain in the database. To remove one or more Dhuma accounts:

1. Check one or more Dhuma accounts you wish to remove.
2. Click Remove and OK to confirm the operation.

4.5 Managing the CA Account Site

Once a CA account has been created, and role certificates have been added to the ACL by an Administrator from the Admin Site, authorized CA account users can manage their account via the CA Account Site.

4.5.1 Logging in the CA Account Site

To access the CertAgent account administration login page for a CA account, launch Firefox and enter the following URL into its address bar:

```
https://<hostname/IP address>:<admin port>/certagentadmin/ca/login.jsp
```

Be sure to replace `<hostname/IP address>` and `<admin port>` with the appropriate system name or IP address and TLS port of your CertAgent webserver. Select your role certificate (*e.g.,* CertAgent *<version>* Administrator) in the security dialog to authenticate yourself to the webserver, and then click **OK**.

A page with an access banner and a Login button will appear. Click **Login**. A welcome page with a drop-down listing the CA accounts that you are authorized to access will appear. Select your desired

CA account. A status page will appear a message: “You are currently logged in as an authorized user (<subject DN of the client certificate>) with <permissions> rights.”

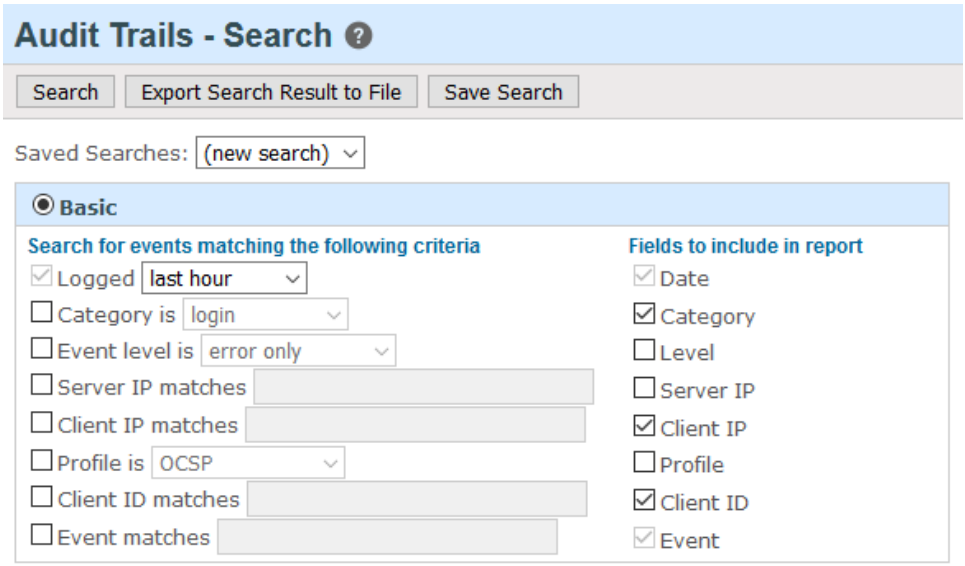
For more information on CA account management and usage, please refer to the on-line help pages:

```
https://<hostname/IP address>:<admin port>/certagentadmin/ca/help.html
```

4.5.2 Searching the Audit Trail

To search the audit trail of a CA account:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your auditor certificate with ‘audit’ permission.
2. In the left panel, click **Search, Audit Trails.**
3. To search the audit trails using the basic search criteria:



Specify the desired search criteria and the fields to be included in the report. You may use an asterisk (*) as a wildcard in the search string.

The descriptions of each setting on this page are given in the following table:

Settings	Description
Date	Timestamp of the event in string Available options: last hour, last 12 hours, today, last 7 days, last 30 days, and custom
Category	Type of the event: request, certificate, CRL, OCSP, user, login, credential, RAMI, DBAccess, config, EST, and audit; If not specified, all types will be displayed
Event level	Level of the event: INFO or ERROR. If specified, either error only and information only can be set. If not specified, both information and error events will be displayed.

Server IP	IP address of the CertAgent system
Client IP	IP address of the client system To search for events triggered by the system, enter [system]. To search for events triggered by the CACLI, installer, startup script, and update tool, enter CACLI, Installer, Startup Script, and Update Tool respectively.
Profile	Profile used in of the event.
Client ID	The identity of the client Subject DN of an authorized user's certificate, EST user name, or CACLI.
Event	Recorded events

TABLE 16 AUDIT TRAIL SETTINGS

4. To search the audit trails using an SQL statement:
   a. Select the **Advanced** option.

      Specify one or more columns to be included in the first text area and optionally specify the WHERE clause in the second text area to construct the desired SQL statement.

   b. Click **Search** to search for the events. The result will be displayed in the **Result** tab.
   c. To export the list of displayed events to a file in CSV format, click **Export Search Result to File**.
5. To save the search to reuse, click **Save Search**.
   a. Select **Save** to overwrite the existing search.
   b. Otherwise, select **Save as** and specify a name.
   c. Click **Save** to apply the changes.

4.5.3 Managing CA Credentials

4.5.3.1 Generating Credential for a Root CA

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Preferences, Credentials.**
3. Click **New Credential**.
4. Select **Generate a new key pair** and **A Root CA, with a self-signed certificate**. Then, click **Next**.
5. Specify the RDNs. If necessary, change the validity period, key type and size, message digest, or certificate extensions, and then click **Generate**. Click **OK** to confirm your intentions.

6. CertAgent will generate a new key pair of the type you specified. Once your new certificate has been installed, its properties will be displayed.

4.5.3.2 Generating Credential for Subordinate CA

Subordinate CA certificate can be issued by an external CA or an internal CA on the same system.

4.5.3.2.1 External CA

If the superior CA that will issue your certificate does not reside on the same system, follow below steps:

To generate the key pair and certificate request:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Preferences, Credentials.**
3. Click **New Credential**.
4. Select **A subordinate CA** and **to be submitted to an external CA** options and click **Next**.
5. Specify the RDNs, and select the key type and size, and message digest.
6. Click **Generate.**
7. Click **OK** in the confirmation dialog.

   CertAgent will:

   - generate a new key pair of the type you specified,
   - create a certificate request containing the public key, and
   - store the HSM access information with the HSM PIN encrypted under the system certificate and certificate request into the database
   - It will then display the properties of the certificate request.
8. Click **Export Request (**and select either the **Binary** or **Base64-encoded** output formats) to save your certificate request to a file that you may manually submit to a superior CA.

To install the certificate and chain:

If your request has been submitted to an external CA and you have obtained the issued certificate and its chain in a PKCS#7 format:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Preferences, Credentials.**
3. Click **Install Certificate**.

4. Click **Browse…** and locate the appropriate PKCS#7 certificate file that includes the issued CA certificate and its chain, then click **Install**.
5. Once your certificate has been validated and installed, a confirmation message and your certificate properties will be displayed.

4.5.3.2.2 Internal CA

If the superior CA that is to issue your certificate resides on the same system, follow below steps:

To generate the key pair and certificate request:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Preferences, Credentials.**
3. Click **New Credential**.
4. Select **A subordinate CA** and **to be submitted to a CA on this system** options and click **Next.**
5. Select the superior CA who is to issue your certificate and complete the Certificate Request Information part of the form.
6. Specify the RDNs, and select the key type and size, and message digest.
7. Click **Generate**.
8. Click **OK** in the confirmation dialog.

   CertAgent will:

   - generate a new key pair of the type you specified,
   - create a certificate request containing the public key, and
   - store the HSM access information with the HSM PIN encrypted under the system certificate, and certificate request into the database

   Your request will then be forwarded to the specified superior CA, and confirmation of the success of this process will be displayed to you on a Results page.

To install the certificate and chain:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your administrator certificate with 'admin' permission.
2. In the left panel, click **Preferences, Credentials.**
3. Click Check **Status**.
4. If your certificate has been issued, its properties will be displayed. Click **Install** to install your certificate in place of the certificate request. If your certificate has *not* yet been issued, you will need to try again later. Contact your superior CA if necessary.

4.5.3.3 Exporting Credentials

Once your CA credentials have been installed, you can export them to a file.

To export the CA credentials:

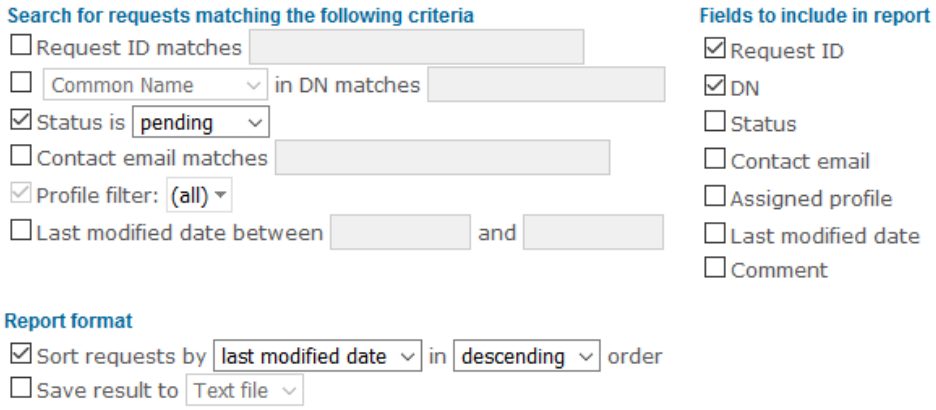
1. Click Preferences, Credentials, then click Export.
2. Click one of the available certificate file formats: binary, base64-encoded X.509 certificate (.der), or PKCS#7 certificates (.p7b).
   For cross certification, select binary or base64-encoded PKCS#10 format. Submit the saved certificate request to the desired Certificate Authority for cross certification.
3. Click [X] to close this dialog.

4.5.4 Managing Certificate Requests

Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'certify' permission.

4.5.4.1 Searching Certificate Requests

1. In the left panel, click **Certificate Requests, Search.**



   a. Specify the desired search criteria (request ID, RDN, status, contact email address, profile filter, and last modified date) to be matched. You may use an asterisk (*) as a wildcard in the search string.

   b. If there are additional profiles associated with your master account, you may allow the query to include one or more profiles by selecting them in the 'Profile filter' drop-down. Otherwise, only certificate requests assigned to the active profile will be returned.

   c. Check the fields to include in the report in the right-hand column.

   d. Specify the report format (sort order, and save option).

2. Click **Search**.

   Once the system has listed the certificate requests matching your search criteria, you may click one to open an **Advanced** functions page; the functions you may perform on a given request will depend upon its current status.

3. To refine your search, select the **Search** tab.

4.5.4.2 Viewing Pending Requests

In the left panel, click **Certificate Requests, Pending.**

4.5.4.3 Issuing Certificates

To issue certificates for one or more pending certificate requests:

1. First, view the pending certificate requests that have been submitted to your account by clicking **Pending** in the **Certificate Requests** section of the navigation panel.

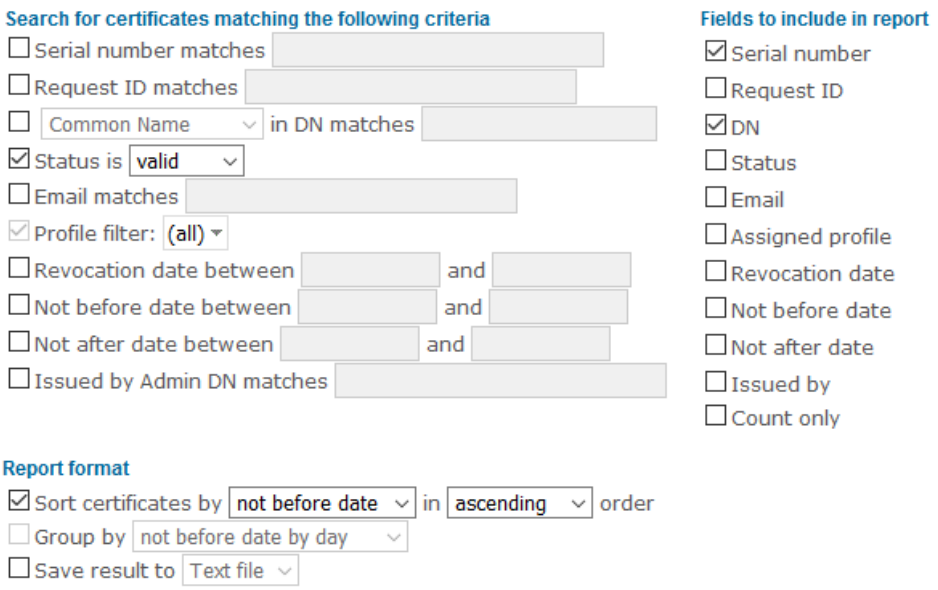
   If there are additional profiles associated with your master account, you may filter the pending requests by profile using the **Active Profile** drop-down list at the top of the page. To view the properties of any request, click the certificate request icon immediately to the right of the corresponding check box. Check **Show details** to view the properties of all displayed requests.

2. If you wish to process one or more certificate requests using the default certificate issuance settings for your account, check the selection boxes next to those you wish to process and click **Issue Selected**. To process a single request, click the **Issue** button adjacent to that request.

4.5.5 Managing Certificates

4.5.5.1 Searching Certificates

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with ‘certify’ or ‘revoke’ permission or Auditor certificate with ‘audit’ permission.
2. In the left panel, click **Certificates, Search**. The following page will appear:



3. Specify the desired search criteria (serial number, request ID, RDN, status, contact email address, profile filter, revocation date, not before date, not after date, and admin DN). You may use an asterisk (*) as a wildcard in the search string.

   If there are additional profiles associated with your master account, you may allow the query to include one or more profiles by selecting them in the '**Profile filter**' drop-down. Otherwise, only the certificates assigned to the active profile will be returned.

4. Check the fields to include in the report in the right-hand column.

   To count the number of certificates matching the search criteria, check the '**Count only**' checkbox and optionally select the group by option to group the result by not before or not after date.

5. Specify the report format (sort order, group by, and save option), and then click **Search**.

   Once the system has listed the certificates matching your search criteria, you may click one of them to open the **Advanced** page and perform various functions with that certificate; which functions are available will depend on the certificates' current status.

6. To refine your search, select the **Search** tab.

7. Optionally, check '**Save result to**' option to export the results to a CSV or text file.

4.5.5.2 Viewing Valid Certificates

To view valid certificates:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'certify' or 'revoke' permission.

2. In the left panel, click **Certificates, Valid**.

A list of all valid certificates issued by the current account will be displayed.
If there are additional profiles associated with your master account, you may view the certificates issued by them by selecting the appropriate profile name in the **Active Profile** drop-down list at the top of the page.

3. Click the small certificate icon immediately to the right of a certificate's selection box to view its properties.
   Alternatively, click **Show details** to view all certificate details.

4.5.5.3 Revoking Certificates

To revoke a certificate:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'revoke' permission.
2. In the left panel, click **Certificates, Valid**.
3. You can revoke multiple certificates simultaneously by checking the boxes next to those certificates and clicking the **Revoke Selected** button. To revoke a single certificate, click the **Revoke** button adjacent to it.

   Alternatively, you can click on a certificate's DN link to open the **Advanced** page.
   In this dialog, select Revoke as the **Action**, specify a **Status** and **Reason** code (see below), then click **Submit.**
   If you are not using the **Advanced** page, specify a **Status** and **Reason** code (see below), then click **Revoke**.
4. To place the selected certificate(s) on hold, select the **On Hold** option and choose one of the following reasons:

None	No reason specified. (Subject's certificate should be rejected until it is removed from this issuer's CRL.)
Call Issuer	This value has application-dependent semantics. (Subject's certificate should be rejected until it is removed from this issuer's CRL.)
Reject	Subject's certificate should be rejected until it is removed from this issuer's CRL.
Pick-up Token	Physically seize the token containing the private key for this certificate, if possible. (Subject's certificate should be rejected and is probably pending permanent revocation.)

To revoke the selected certificate(s), select **Revoke,** and choose one of the following reasons:

Unspecified	No reason specified. Use of this value is deprecated; choosing "No Reason" to omit a reason code is preferred in most applications.
Key Compromise	The subject's private key is known, or suspected, to have been compromised.
CA Compromise	The subject CA's private key is known or suspected to have been compromised.
Affiliation Changed	Some subject information in the certificate has changed.
Superseded	The certificate has been superseded, perhaps by another certificate containing the same public key, but with a later expiration date.
Cessation of Operation	The certificate is no longer needed for the purpose for which it is originally issued.
Remove from CRL	The entry appears on a previous CRL with reason *certificateHold* but is

	now valid.
Privilege Withdrawn	The privilege contained in the certificate has been withdrawn.
AA Compromise	Aspects of the AA validated in the attribute certificate have been compromised.

5. The certificate(s) will be placed on hold, revoked, or merely marked for revocation, and the results are displayed.

   If the "Support 'pending revocation' as a separate certificate status value" option is 'disabled' (as it is by default), certificates, when initially designated as 'revoked' by a CA, are immediately moved to a 'revoked certificates' list.
   If, however, "Support 'pending revocation' as a separate certificate status value" is 'enabled', certificates are first moved to a list of certificates 'pending revocation'. Certificates pending revocation can be reinstated at any time prior to issuance of a CRL (in which they appear), but once such a CRL has been issued, they are moved to the 'revoked certificates' list.

   NOTE: Only certificates with a status of 'on hold' can be reinstated from the 'revoked certificates' list.

4.5.5.4 Viewing Revoked Certificates

To view the revoked certificates:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'certify' or 'revoke' permission.
2. In the left panel, click **Certificates, Revoked.**

   You may view the properties of a particular certificate in this list by clicking its DN link to open the **Advanced** properties page.

4.5.6 Managing CRLs

Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'revoke' permission

4.5.6.1 Issuing a CRL

To issue a new CRL:

1. In the left panel, click **CRLs, Issue**. Only newly revoked certificates which have not been included in a CRL will be displayed; previously revoked certificates will be included in the CRL but not displayed.
2. Click **Issue CRL**.
3. Click **OK** to confirm this operation.

   A CRL that includes all certificates pending revocation, all on hold certificates, and all previously revoked certificates will be created. Once the operation has been completed, you will be informed of its status.
   You may click the new CRL's **Effective Date** to view its properties in detail or click **Download** to save the new CRL to a local disk file on your computer.

4.5.6.2 Viewing CRLs

To view, inspect, or download an issued CRL:

1. In the left panel, click **CRLs, View**.

   At first, only the most recent CRL will be displayed. If you wish to display a list of all CRLs for your account, click **Show All CRLs**.

2. Click **Download** to save one of the CRLs to a local disk file on your computer.

3. You may also click a CRL's **Effective Date** to view its properties in detail. Click **Close** when you are ready to close the properties dialog.

4.5.7 Managing Account Preferences

Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your Administrator certificate with 'admin' permission.

4.5.7.1 Managing Certificate Enrollment

CertAgent supports the enrollment of users via a web browser, Enrollment over Secure Transport (EST) and from Registration Authorities (RAs) through the Registration Authority Management Interface (RAMI).

To manage certificate enrollment settings, click **Enrollment** in the **Preferences** section of the navigation panel. Select one of the following tabs to configure its settings and click **Apply** to save your changes.

4.5.7.1.1 Configuration

Acceptable key types and sizes can be configured on this page. By default, only RSA 3072 or above, and elliptic curves NIST P-256 and NIST P-384 are accepted.

Select the acceptable key types and sizes as appropriate for your requirement. If a received certificate request does not meet the specified requirements, it will be automatically rejected.

NOTE: Settings in this page are profile-based. If there are additional profiles associated with your master account, you may manage the profile's settings using the **Active Profile** drop-down list at the top of the page.

4.5.7.1.2 Web

This page controls the settings on the public site's 'Upload Request' and 'Enroll using Browser' pages.

The settings you can control on this page are:

Enable this profile in enrollment page	If checked, user can generate a key pair in a browser and submit a certificate request to this account or profile.

Internet Explorer options	You can set and/or enforce the choice of **CSP** and **KSP**, as well as the **Strong private key protection** and **Mark keys as exportable** options so that they are suggested to (or forced on) users when they use Internet Explorer to generate and submit a certificate request.
Enable this profile in upload page	If checked, user can submit PKCS#10 request to this account or profile.
Comment Field	If enabled, a user comment field will appear on the certificate enrollment or upload form.
Contact Email	You can specify the number of email address fields to display on the form and number of email addresses required to be specified by users.

NOTE: Settings in this page are profile-based. If there are additional profiles associated with your master account, you may manage the profile's settings using the **Active Profile** drop-down list at the top of the page.

4.5.7.1.3 EST (Enrollment over Secure Transport)

CertAgent supports Enrollment over Secure Transport (EST) protocol as described in RFC 7030 to receive and act upon certificate enrollment requests using the simple enrollment method described in RFC 7030 Section 4.2. Certificate enrollment requests are authenticated using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2, authenticated using a username and password as specified by RFC 7030 Section 3.2.3, or authenticated using a special RA certificate issued by the CA and asserting the id-kp-cmcRA OID in its extended key usage extension as specified by RFC 7030 Section 3.7.

CertAgent supports the following EST operations, authentications, and URLs:

Operation	Authentication	URL Format
Distributions of CA certificates	None	https://<host>:<public port>/.well-known/est/<ca>/cacerts https://<host>:<public port>/.well-known/est/cacerts
Enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/<ca>/simpleenroll https://<host>:<admin port>/.well-known/est/simpleenroll
	Basic	https://<host>:<public port>/.well-known/est/<ca>/simpleenroll https://<host>:<public port>/.well-known/est/simpleenroll
Re-enrollment of clients	Certificate-based	https://<host>:<admin port>/.well-known/est/<ca>/simplereenroll https://<host>:<admin port>/.well-known/est/simplereenroll
	Basic	https://<host>:<public port>/.well-known/est/<ca>/simplereenroll https://<host>:<public port>/.well-known/est/simplereenroll

TABLE 17 EST OPERATIONS, AUTHENTICATIONS, AND URL FORMATS

The CA account or profile in which the requests are submitted is specified in the <ca> path segment in the EST URL. If a default EST account has been configured by the administrator of the System

Administrative site, the URLs without the <ca> path segment will also be supported. In the evaluation, only the URLs containing the <ca> path segment will be used.

For basic authentication, the user name must match the common name in the subject DN, or RFC822 name or DNS name in the subject alternative name of the certificate request.

NOTE: Authorized EST users are managed by CA Operations Staff. For details, see section *4.5.7.9.2 EST (Enrollment over Secure Transport) Users*.

For certificate-based authentication, the client's certificate must pass the path validation and trusted by the web server. If the client's certificate is issued by the EST CA and includes the id-kp-cmcRA (1.3.6.1.5.5.7.3.28) purpose in the extended key usage extension, the client is a Registration Authority (RA). An RA can submit any certificate requests via EST. If the client is not an RA, the common name in the subject DN and the subject alternative name included in the client certificate must match the ones in the certificate request.

CertAgent treats EST re-enrollment operation the same as enrollment. Authorized users or RAs can submit their EST requests to either operation.

The set of supported ciphersuites (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, and TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA) is the same as the TOE.

To enable EST:

1. Check **Enable EST** checkbox and click **Apply**.
2. The URLs to access the EST interface will be displayed.

CertAgent supports both POST and GET HTTP protocols for EST operations. EST requests can be submitted from EST client or any programs that can submit POST and/or GET requests (e.g., curl).

To submit a CA certificate request:

1. Either submit a POST or GET request to the following URL from your EST client:

   ```
   https://<host>:<public port>/.well-known/est/<ca>/cacerts
   ```

2. A base64-encoded CA certificate and its chain in a PKCS#7 format will be returned in the response with HTTP 200 response code, `Content-Type: application/pkcs7-mine;smime-type=certs-only`, and `Content-Transfer-Encoding: base64` headers.

To submit a certificate enrollment request:

1. Submit a POST request with `Content-Type:application/pkcs10` header and base64-encoded certificate request in the content to one of the enrollment URL from an EST client.

2. To submit a POST request using curl, run one of the following commands as appropriate for your authentication:

```
# use basic authentication
# as a subscriber
curl <url> --basic –u "<username>:<password>" –v –o <out p7 file> --cacert
<SSL trust root> --data-ascii @<base64-encoded PKCS#10 file> -H "Content-
Type: application/pkcs10" --tlsv1.1

# use client authentication
# as an RA or a subscriber
# convert user's PKCS#12 to PEM format and don't encrypt the private key
openssl pkcs12 –in <p12 file> -out <out pem file> -nodes
curl <url> --cert <out pem file> -v –o <out p7 file> --cacert <SSL trust
root> --data-ascii @<base64-encoded PKCS#10 file> -H "Content-Type:
application/pkcs10" --tlsv1.1
```

3. If the enrollment is successful, the issued certificate in a PKCS#7 format will be returned in the response with HTTP 200 response code, `Content-Type: application/pkcs7-mine`, and `Content-Transfer-Encoding: base64` headers.

   Otherwise, one of the HTTP response codes (400: bad request, 404: page not found, or 500: internal server error) will be returned along with the detailed error message in the response.

4.5.7.2 RAMI (Registration Authority Management Interface)

The CertAgent Registration Authority Management Interface (RAMI) allows a remote or automated client process (acting on behalf of an authorized registration authority) to:

- submit a certificate request for immediate processing and obtain an issued certificate;
- revoke a certificate;
- reinstate a certificate with a status of on-hold or pending revocation;
- issue a CRL;
- retrieve the CA accounts information;
- query certificate request information;
- query certificate information;
- and retrieve an issued certificate

over a TLS-secured connection (with client authentication).

To manage the RAMI settings, click **RA Management** in the **Preferences** section of the navigation panel.

Depending on the privileged user's role and permission, the options available in this page are appropriately limited.

The settings in which a user with 'certify' permission can control on this page are:

Allow certificate enrollment	Enabling this option allows an authorized registration authority (RA), possibly an automated process acting on behalf of the CA, to submit certificate requests and obtain certificates over an SSL connection with client authentication. This option applies to all profiles.
Allow certificate request and certificate queries	Permits certificate request and certificate queries via RAMI when checked. This option applies to all profiles.

The settings in which a user with 'revoke' permission can control on this page are:

Allow CRL issuance	Permits CRL issuance via RAMI when checked. This option applies to all profiles.
Allow certificate revocation and reinstatement	Permits certificate revocation and reinstatement via RAMI when checked. This option applies to all profiles.

The settings in which a user with 'admin' permission can control on this page are:

Allow POST to override default CRL settings	If checked, authorized RAs may use POST parameters to override the CRL issuance settings. This option is available if 'Allow CRL issuance' is enabled and applies to all profiles.

Click **Apply** to save your changes.

For details on submitting RAMI requests, see section *4.7 Using RAMI*.

4.5.7.3 Managing Certificate Profiles

A master CA account can have one or more profiles with their own account IDs and access control lists (administered by a user of the master account with 'admin' permission). While each profile shares its credentials with the master CA account, each profile can have its own default settings for certificate issuance, *etc.* In this way, a master CA can delegate to subordinates the issuance of certificates (and possibly CRLs) with varying default attributes and extensions but the same issuer keys.

To create a new profile:

1. In the left panel, click **Preferences, Certificate Profiles.**
2. Click **Create**.
3. Enter the Profile ID and display name, then click **Create.**

Profile ID	A unique identifier for this profile; may only contain the characters A-Z, a-z, and 0-9.
Display Name	The friendly name of the profile; may only contain the characters A-Z, a-z, 0-9, and space.
Copy Setting from	If '(none)' is selected, the default configuration will be assigned to the new profile. Otherwise, the configuration of the selected profile will be copied to the new profile.

4. Click **OK** to confirm the operation.

   A profile will be created with the specified profile ID. This profile will share credentials with its master account (*i.e.*, the master account and all profiles use

the same key pair for issuing certificates and CRLs). However, each profile has its own certificate issuance, enrollment, and email settings, and a separate access control list.

To remove a profile from the system:

1. In the left panel, click **Preferences, Certificate Profiles.**
2. Select the master profile from the Active Profile drop-down list at the top of the page.
3. Check one or more profile you wish to delete from the list, then click **Remove**.
4. Click OK to confirm the operation.

To modify the settings for a profile:

1. In the left panel, click **Preferences, Certificate Profiles.**
2. Select the profile you wish to modify from the **Active Profile** drop-down list at the top of the page.
3. To change the display name:
   a. Select the **Display Name** tab to change the profile name and rights as desired
   b. Click **Apply** to save your changes.
4. To manage the profile access control list:
   a. Select the Access Control List tab. The certificates of all users authorized to use this profile are displayed.
   b. To add a certificate to the list, click **Add**. Then upload the certificate by clicking **Browse…**, locating the appropriate certificate file, selecting the desired permissions, and clicking **Upload**. A confirmation message will be displayed, and the certificate will appear in the access control list if the operation is successful.
5. To remove one or more certificates from the ACL:
   a. Check the box before each certificate you wish to delete and click **Remove**.
   b. Click **OK** in the confirmation dialog to remove the selected certificate(s) from the profile ACL.

4.5.7.4 Managing Certificate Issuance

To change the certificate issuance options for an account, click **Preferences, Certificate Issuance.** Select one of the following tabs to configure its settings and click **Apply** to save your changes.

If you are logged in as an authorized user with ‘certify’ permission only, the option you can control on this page is:

Automatically issue certificates upon request	To enable automatic certificate issuance, check this box.

If you are logged in as an authorized user with 'admin' permission, you will be presented with a page containing the Properties, Extension, Filter, and Serial No. tabs. The sections below describe the settings on each tab.

4.5.7.4.1 Properties

The **Properties** tab displays the default settings for issuing certificates. The options you can control on this page are:

Class 1 Assurance	For email-based end-user identity proofing. If checked, every certificate request must contain the submitter's email address; otherwise, it will be rejected. The requester will not receive a Request ID after enrollment, rather an email notification containing a retrieval URL will be sent to him once the certificate request has been processed. Certificates are only considered valid once they have been retrieved via these emailed links.
RDNs	Each specified RDN has a default value and an inclusion setting: Require: Use the value found in the request; the user must enter a value for this RDN on the public Enrollment page. Allow: Use the value found in the request; the specified default value is displayed on the public Enrollment page, but the user is allowed to change it. Force: Always use the specified value; it displays on the public Enrollment page, and the user cannot change it. When issuing certificates for this account, CertAgent will include the available RDNs in the specified order. Use the  button to add an RDN component below the current RDN. Use the  button to delete the current RDN. Use the  button to move the current RDN up. Use the  button to move the current RDN down. If the internal LDAP repository for your CA account is enabled by the site administrator, make sure your default RDN settings agree with the configured LDAP search base. For example, if the search base is set to 'O=ISC, C=US', the default settings for certificate issuance should include the 'forced' RDNs 'O=ISC' and 'C=US'. All issued certificates must have subject DNs ending with the search base criteria to be returned in response to queries to the internal LDAP server.
Encoding	Encoding of DNs: PrintableString (default) or UTF8String.
Validity Period	Specify the default validity period for issued certificates.
Message Digest	One or more of the following message digest algorithms are available: SHA-384 and SHA-512. Certificates will be signed using the specified message digest. The most appropriate choice depends on the size and type of the CA's credentials.

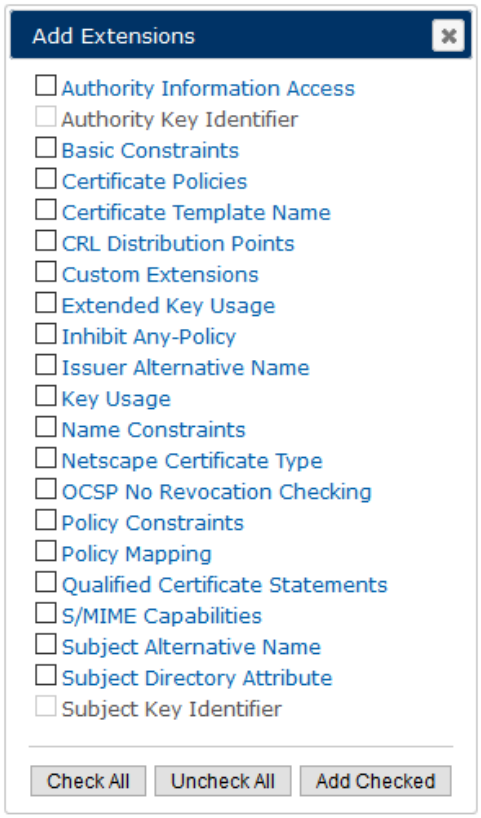
Modify any settings you wish to change in the **Properties** pages, then click **Apply.**

4.5.7.4.2 Extensions

The **Extensions** tab displays the default certificate extension settings.

To add extensions:

1. Click **Add Extensions**. A list of supported extensions will be displayed:



2. To add a single extension and close this dialog, just click on its link. To add multiple extensions, check them and click **Add Checked**.

To remove extensions:

1. Click the **[X]** to the right of the extension name.
   Brief descriptions of all supported extensions are given in the following table. Each of these extensions is flagged as critical if the associated Critical checkbox is set.

Extension	Description
Authority Information Access	This extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Available access methods are CA Issuer, CA OCSP, and user specified OID.
Authority Key Identifier	This extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. Available identifier types: key ID, CA issuer DN, and issuer serial number. NOTE: If 'Require authorityKeyIdentifier extension' option is enabled in the Admin Site, this extension cannot be removed from the default extension list, and all certificates to be issued must include this extension.
Basic Constraints	This extension indicates whether the subject can act as a CA or is only an end-user entity. It is added to every certificate issued by CertAgent. This extension is flagged as critical if the Critical checkbox is set. If you are a root CA whose sole (or principal) role is to certify the public keys of

	subordinate CAs (as opposed to end-users), you should set the CA certificate checkbox (and optionally select a default pathLength value). On the other hand, if you typically issue end-user certificates, leave this box unchecked. The Path length setting, if one is selected, indicates to consumers of the certificate that they should not accept a certificate path whose length exceeds the specified value by more than one. For example, if the pathLength attribute is set to 2, users should not accept as valid chains containing more than three certificates.
Certificate Policies	This extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional policy qualifiers (CPS and user notice).
Certificate Template Name	This extension contains the certificate template name.
CRL Distribution Points	This extension identifies how CRL information is obtained. URL (e.g., LDAP and HTTP URL) and DN forms are accepted.
Custom Extension	To add an extension that is not explicitly supported by CertAgent, enter the base64-encoded extension data into the text box.
Extended Key Usage	This extension indicates one or more purposes for which the certified public key may be used in addition to, or in place of, the basic purposes indicated in the key usage extension. See the following table for details.
Inhibit Any-Policy	This extension indicates that the special anyPolicy OID, is not considered an explicit match for other certificate policies. The value indicates the number of additional certificates that may appear in the path before anyPolicy is no longer permitted.
Issuer Alternative Name	This extension allows alternative names to be bound to the issuer of the certificate. Supported name forms include: rfc822Name, otherName, dNSName, DN, URL, IPAddress, ediPartyName, registeredID, and x400Address. If 'Octet String' type is selected for otherName, its value can be a text string or hex-encoded string starting with '0x'; otherwise, the value can be a text string or UTF8 string. To include an x400Address value, enter the desired base64-encoded value into the supplied text box.
Key Usage	An extension that indicates the intended purpose of the subject public key inside the certificate. Select usage settings in accordance with your current certificate authority policy, taking into account the type of the public keys you will most likely be asked to certify. (See definitions below.) The "recommended" keyUsage setting for end-user certificates is "digital signature + non-repudiation + key encipherment + key agreement." For CA certificates it is "certificate signing (mandatory) + CRL signing (mandatory)." If the Critical checkbox in this section is set, and this extension is to be added to a certificate, it will be flagged as critical. Turn criticality on if use of the subject's public key for a purpose other than that indicated by the selected keyUsage bits would constitute a violation of your certificate authority policy.
Name Constraints	This extension is used only in CA certificates. It indicates a name space within which all subject names in subsequent certificates in a certification path must be located.
Netscape Certificate Type	This is a Netscape specific extension that can be used to limit the applications for a certificate. Available types are: SSL client certificate, SSL CA certificate, SSL server certificate, S/MIME user certificate, S/MIME CA certificate, object signing certificate and object signing CA certificate.
OCSP No Revocation	This extension is used only in an OCSP signing certificate. If this extension is included,

Checking	no revocation checking is to be performed on the OCSP signing certificate during OCSP operations.
Policy Constraints	This extension can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier. If require explicit policy is set, the value indicates the number of additional certificates that may appear in the path before an explicit policy is required for the entire path. If inhibit policy mapping is set, the value indicates the number of additional certificates that may appear in the path before policy mapping is no longer permitted.
Policy Mapping	This extension is used only in CA certificates. It lists one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy. The pairing indicates that the issuing CA considers its issuerDomainPolicy equivalent to the subject CA's subjectDomainPolicy.
Qualified Certificate Statements	This extension is the inclusion of statements defining explicit properties of the certificate. Available statements are: Financial limit clause (id-etsi-qcs-QcLimitValue), ETSI TS 101 862 authentic certificate clause (id-etsi-qcs-QcCompliance), NES telecommunication agency authentic certificate clause and retention period (id-etsi-qcs-QcRetentionPeriod).
S/MIME Capabilities	This extension indicates cryptographic capabilities of the sender of a signed S/MIME message.
Subject Alternative Name	This extension allows alternative names to be bound to the subject of the certificate. Supported name forms include: rfc822Name, otherName, dNSName, DN, URL, IPAddress, ediPartyName, registeredID, and x400Address. If the appropriate RFC822 name options are checked and email address in the subject DN is set and /or contact email addresses are specified, they will be included in this extension. If 'Octet String' type is selected for otherName, its value can be a text string or hex-encoded string starting with '0x'; otherwise, the value can be a text string or UTF8 string. To include an x400Address value, enter the desired base64-encoded value into the supplied text box. If 'Accept values from the public enrollment page' checkbox is checked, select one or more of the supported names. Selected names will be appeared in the public enrollment page and user can specify the values if needed. If 'Enable DNS name filter' checkbox is checked, specify one or more DNS name patterns to be rejected or allowed.
Subject Directory Attribute	This extension is used to convey identification attributes of the subject. Available attributes are country of citizenship (US DOD), country of citizenship (RFC 3739), employee type and nationality.
Subject Key Identifier	This extension provides a means of identifying certificates that contain a particular public key.

TABLE 18 EXTENSIONS

Brief descriptions of the options in the keyUsage are given in the following table:

CertAgent Option	Description
digital signature	The subject public key may be used to validate signatures used for purposes other than non-repudiation and signing certificates/CRLs.

non-repudiation	The subject public key may be used to validate signatures used in non-repudiation services.
key encipherment	The subject public key may be used to wrap a (symmetric) session key for the purpose of key transport.
data encipherment	The subject public key may be used for bulk data encryption.
key agreement	The subject public key may be used in a key agreement protocol.
certificate signing	The subject key may be used to validate signatures on certificates. This bit cannot be set for end-user certificates and must be set for CA certificates.
CRL signing	The subject public key can be used to validate the signature on a certificate revocation list (CRL). This bit can only be set for CA certificates.
encipher-only	The subject key can only be used for encryption as part of a key agreement protocol. Should be used only in conjunction with the key agreement option.
decipher-only	The subject key can only be used for decryption as part of a key agreement protocol. Should be used only in conjunction with the key agreement option.

TABLE 19 KEY USAGE EXTENSION

Brief descriptions of the key purpose identifiers and other attributes that may be included in the Extended Key Usage (EKU) extension are given in the following table:

Identifier	Description
server authentication	The subject public key may be used for TLS WWW server authentication.
client authentication	The subject public key may be used for TLS WWW client authentication.
code signing	The subject public key may be used for signing of downloadable executable code.
email protection	The subject public key may be used for email protection.
time stamping	The subject public key may be used for binding the hash of an object to a time.
Microsoft: encrypted file system	The subject public key may be used for Microsoft's encrypted file system.
PIV Card Authorization	This subject public key may be used for PIV Card authorization.
Microsoft Smart Card Logon	This subject public key may be used for Microsoft's smart card logon.
OCSP signing	This subject public key may be used for signing by an OCSP responder; see RFC 2560.
IPSec IKE	This subject public key may be used for IPSec IKE (old OIDs have been deprecated).
IPSec end system	This subject public key may be used for an IPSec end system.
IPSec tunnel	This subject public key may be used for IPSec tunneling.
IPSec user	This subject public key may be used for an IPSec user.
extensible authentication	This subject public key may be used for EAP over LAN.

protocol over LAN	
extensible authentication protocol over PPP	This subject public key may be used for EAP over PPP; see RFC 2284.
SCVP responder	This subject public key may be used for an SCVP responder.
SCVP server	This subject public key may be used for an SCVP server.
SCVP client	This subject public key may be used for an SCVP client.
data validation and certification server	This subject public key may be used for a data validation and certification server.
CMC Registration Authority	This subject public key may be used for Certificate Management over Cryptographic Message Syntax (CMC) Registration Authority (RA).
accept any	This subject public key may be used for any usages.
user-defined OIDs	One or more user-defined OIDs (specified in standard 'dot notation' may be included in a certificate's extendKeyUsage extension.

TABLE 20 EXTENDED KEY UAGE EXTENSION

If 'Require consistent values in keyUsage and extendedKeyUsage' option is enabled in the Admin site, the following purposes in the extended key usage extension must be set with the specified purpose in the key usage extension:

- Server authentication (1.3.6.1.5.5.7.3.1) must be set with digital signature, key encipherment or key agreement
- Client Authentication (1.3.6.1.5.5.7.3.2) must be set with digital signature and/or key agreement
- Code signing (1.3.6.1.5.5.7.3.3) must be set with digital signature
- Email protection (1.3.6.1.5.5.7.3.4) must be set with digital signature, non-repudiation, and/or (key encipherment or key agreement)
- Time stamping (1.3.6.1.5.5.7.3.8) must be set with digital signature and/or non-repudiation
- OCSP signing (1.3.6.1.5.5.7.3.9) must be set with digital signature and/or non-repudiation

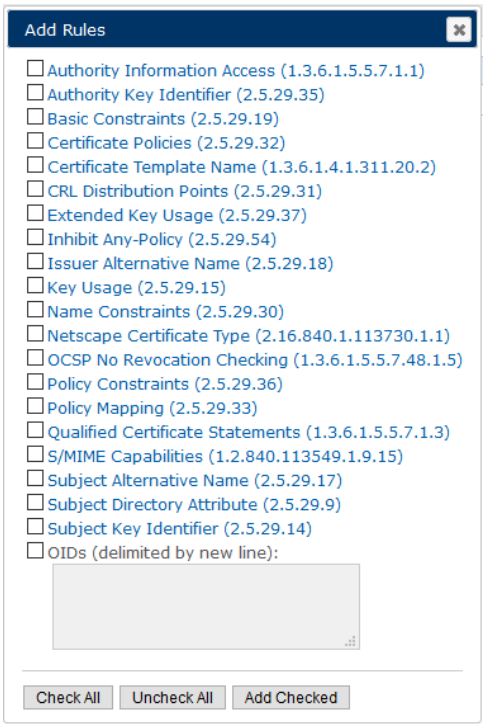
Modify any settings you wish to change in the **Extensions** pages, then click **Apply.**

4.5.7.4.3 Filter

The **Filter** tab displays the rules for processing certificate requests. By default, all extensions in submitted certificate requests are omitted from the issued certificates. To accept and pass through certain extensions, rules for their handling must be explicitly defined.

To add rules:

1. Click **Add Rules**. A list of extensions will be displayed.



2. To add a single extension and close the dialog, click on its link. To add multiple extensions, check them and click **Add Checked**. To add extensions that are not explicitly supported, check the OIDs checkbox and enter a list of extensions in the text box.

3. Modify the handling of each newly added extension by appropriately setting the corresponding action value. Brief descriptions of the available action values appear in the following table:

Action	Description
Require	This extension is required. If a submitted request doesn't contain this extension, it is automatically rejected. By default, this extension is included in the certificate, and the default value specified in the Extension tab is ignored. NOTE: This option is not available for Key Usage and Extension Key Usage extensions.
Require and Match Profile	This extension is required. If a submitted request doesn't contain this extension or the specified extension doesn't match the specified purpose of the extension, it is automatically rejected. NOTE: This option is only available for Key Usage and Extended Key Usage extensions.
Allow	This extension is optional. If it appears in a request, it is included in the certificate. Otherwise, the default value specified in the Extension tab is applied.
Omit	This extension, if present in a request, is ignored. The default value specified in the Extension tab is applied.
Flag	If this extension is found in a request, the request is flagged with a warning notation. Manual issuance of the certificate is required.

Reject	If this extension is found in a request, the request is automatically rejected.

TABLE 21 FILER ACTIONS AND DESCRIPTIONS

4. Modify any settings you wish to change in the **Filter** pages, then click **Apply.**

To remove an extension processing rule:

1. Click the **[x]** to the right of the extension name.
2. Modify any settings you wish to change in the **Filter** pages, then click **Apply.**

4.5.7.5 Managing CRL Issuance

To change the CRL issuance options for an account:

1. In the left panel, click **Preferences, CRL Processing.**
2. If you are logged in as a CA Operations Staff with 'revoke' permission, the options you can control on this page are:

Issue CRL automatically	If enabled, CertAgent will issue a CRL automatically at the specified frequency. This frequency must not be greater than the CRL validity period.
Issue CRL automatically for every certificate revoked with one of the following reasons	If enabled, CertAgent will issue CRLs automatically whenever the CA revokes, or places on hold a certificate with the specified reason code.
Issue CRL automatically for every on hold certificate reinstatement	If enabled, CertAgent will issue CRLs automatically whenever the CA reinstates an on-hold certificate.

3. If you are logged in as an Administrator, the options you can control on this page are:

CRL validity period	This time period will be added to the current date to provide the *nextUpdate* field for each CRL that is issued.
Message Digest	CRLs are signed using the specified message digest algorithm. The digital signature is used to provide proof of origin. The most appropriate choice depends on the size and type of the CA's credentials. One or more of the following message digests are available: SHA-384 and SHA-512.
Exclude reason code in revoked certificate list	If enabled, the reason code of the revoked certificates will not be included in the CRLs.
Archive only the latest CRLs	If enabled, CertAgent will keep at most the specified number of CRLs in the database. Once the maximum number of CRLs has been issued, older CRL are removed from the database as newer ones are issued.
Authority Key Identifier	This extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. This extension is flagged as critical if the **Critical** checkbox is set.
CRL Number	This extension conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer. This extension is flagged as critical if the **Critical** checkbox is set.

4. To include an Authority Key Identifier and/or CRL number extensions in a CRL, click **Add Extensions**. Check the desired extensions and click **Add Checked**.
5. Edit these settings as desired, then click **Apply**.

4.5.7.6 Managing OCSP Responder Settings

CertAgent supports Online Certificate Status Protocol (OCSP). OCSP requests must contain only one target certificate identifier with or without nonce. Requests must be submitted via HTTPS or HTTP POST with `Content-Type` header set to `application/ocsp-request` to the following URL:

```
http[s]://<host>:<port>/certagent/ocsp/<ca name>
```

If the URL is valid and OCSP is enabled for the specified CA account, CertAgent will construct and sign the response by a delegated OCSP signer or the same private key of the CA account which signs certificates and CRLs. The `Content-Type` header of the HTTP response will be set to `application/ocsp-response`.

To enable OCSP Responder for an account:

1. In the left panel, click **Preferences, OCSP Responder**.
2. Check the **Enable OCSP Responder** checkbox.
   The options you can control on this page are:

Response caching	If enabled, the OCSP response without a nonce will be cached and reused for the same request. This option applies if the request does not have a nonce or the 'Exclude a nonce in the response' option is enabled.
nextUpdate field	nextUpdate field in the OCSP response. Available options: • Same as CRL's nextUpdate • Specify a time period from thisUpdate field
nonce field	Nonce field in the OCSP response. Available options: • Include the same nonce if found in the request • Exclude a nonce in the response • Reject the request with a nonce
Hash algorithm	Hash algorithm to sign the OCSP response. Available options: • SHA-1 • SHA-256 • SHA-384 • SHA-512

3. Edit these settings as desired, then click **Apply**.

4.5.7.6.1 Updating OSCP Signer Credential

To update the OCSP Signer credential, in the left panel, click **Preferences**, **OCSP Responder**. Click **Update Credential**. The Wizard guides you through the process of updating the OCSP signer credential for your CA account. The remainder of this section explains in greater detail how to use the wizard.

4.5.7.6.1.1 Using the CA Credential

To use the same CA credential to sign OCSP responses:

1. Select 'Use the credential' option. Then, click **Next**.

2. Click **OK** to confirm your intentions. Properties of the CA certificate will be displayed to confirm that it has been successfully assigned to your account.

4.5.7.6.1.2 Generating a New Delegated Signer Credential

To generate a new delegated credential to sign OCSP responses:

1. Select 'Generate a new delegated credential'. Then, click **Next**.
2. Select 'Use default' to use the existing HSM access settings. Otherwise, select 'Use custom' and specify the required HSM access settings. To view the slots and labels available on your HSM, enter the path of the vendor-provided access library and click View Slots/Label. Then, click Next.
3. Specify the RDNs. If necessary, change the encoding of DN, key type, and message digest.
4. Click **Generate**. Then, click **OK** in the confirmation dialog.
   CertAgent will:
   - generate a new key pair of the type you specified,
   - create a certificate request containing the public key,
   - submit the request to the selected profile, and
   - store the HSM access information with the HSM PIN encrypted under the system certificate, and certificate request into the database
5. Properties of the certificate request and status message will be displayed to confirm that it has been successfully submitted to the profile.

Once the certificate request has been submitted, you can check the status of the certificate from the OCSP Responder page.

If your certificate has *not* yet been issued, you will need to try again later. Contact your CA Operations Staff of the CA account if necessary.

If your certificate has been issued, its properties will be displayed. Click **Install** to install your certificate in place of the certificate request. Click **OK** in the confirmation dialog.

4.5.7.6.1.3 Using an Existing Delegated Signer Credential

To use an existing delegated credential:

1. Select 'Use an existing delegated credential'. Then, click **Next**.
2. All available delegated OCSP credentials will be listed.
3. Select the credential you wish to use. (To view detailed information about any of the available certificates, click its DN.) Then, click **Next**.
4. Click **OK** in the confirmation dialog.

   Properties of the selected credential will be displayed to confirm that they have been successfully assigned to your account.

4.5.7.7 Managing Public Site Configuration Settings

To change configuration settings for the public site:

1. Click **Public Site** in the **Preferences** section of the navigation bar.
   The options you can control on the Main page are:

Display Name	Display name will be displayed in the public site as your identification.
Add display name to the drop-down list…	If checked, the specified display name will appear in the drop-down list of CAs on the main page; if unchecked, users will only be able to access the CA resources and services using direct URLs that you must provide privately.

   The options you can control on the CA Resources page are:

Include this page…	If checked, the `CA Resources` page will appear on the public site.
Description	The string you enter will be displayed on the Public site's `CA Resources` page.
Superior CA's CRL URLs	If you are operating as a subordinate CA, you can specify your superior CA. These URLs will be displayed in the `CA Resources` page on the public site.

   The option you can control on the Browser Enrollment, PKCS#10 Enrollment, Search Certificates, and Certificate Revocation page is:

Include this page…	If checked, the specified page will appear on the public site.

   The options you can control on the Certificate Retrieval page are:

Include this page…	If checked, the `Certificate Retrieval` page will appear on the public site.
Text (top)	The specified message will be displayed at the top of the `Certificate Retrieval` page.
Text (bottom)	The specified message will be displayed at the bottom of the `Certificate Retrieval` page

2. Click **Apply** to accept any changes you have made.

4.5.7.8 Managing Revocation Policy

To change the Certificate Management options for an account:

1. Click **Revocation Policy** in the **Preferences** section of the navigation bar.
   The only option you can control on this page is described in the following table:

Support ‘pending revocation’ as a separate certificate status value	If 'disabled', certificates, when initially designated as 'revoked', are immediately moved to a 'revoked certificates' list, and only those with 'on hold' status can later be reinstated. If this option is 'enabled', certificates, when initially flagged as revoked, are first moved to a list of certificates 'pending revocation' from which they can be reinstated at any time prior to issuance of a CRL (in which they'll appear). Once a CRL containing them has been issued, they are moved to the revoked certificates list from which only 'on hold' certificates can be reinstated. Motivation: enabling this option allows the CA to change his mind about certificates tagged for revocation and more closely conforms to an X.509/RFC 3280 convention according to which a certificate is not to be considered ‘revoked’ until it appears on at least one CRL.

2. Edit this setting as you wish, then click **Apply**.

4.5.7.9 Managing Self-Service Settings

4.5.7.9.1 Certificate Revocation

CertAgent supports self-service certificate revocation for users. If enabled, the ‘Revoke’ option will appear in the Main page of the Public Site. Users with valid client certificates issued by the selected CA account can authenticate to the revocation page via TLS client authentication. If authenticated, all the certificates matching the subject DN of the client certificate will be listed. Users can inspect the certificates and select one or more certificates to be revoked with a specified reason code. Once the revocation request has been submitted, selected certificate(s) will be revoked immediately.

NOTE: Only a CA Operations Staff member with ‘revoke’ permission can manage this service.

To enable this service:

1. Click Self-Service in the Preferences section of the navigation panel.
2. Check ‘Allow subscribers to revoke their certificates via the Public Site’ checkbox.
3. Click Apply to save your changes.

4.5.7.9.2 EST (Enrollment over Secure Transport) Users

In cases where the entity requiring a certificate does not have a valid certificate to use for authentication, EST basic authentication is used. In order for an entity to enroll via EST using basic authentication, a CA Operations Staff member with ‘certify’ permission of the CA account must add the common name of the subscriber to the EST list and create an EST password. They then have to pass the EST subscriber name and password information to the subscriber. EST passwords must be at least 15 characters in length and be composed of any combination of upper and lower case letters, numbers, and at least one of the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

When a subscriber connects to the TOE using EST basic authentication, it passes the subscriber name and password to the TOE. The TOE then computes the check value for the presented password and compares it to the value in the database for the supplied subscriber name. If the values match, the subscriber name used matches one of the fields below, the profile allows EST, the username and

password haven't already been used to obtain a certificate, and all other profile compliance checks pass, a certificate will be issued to the entity automatically. The subscriber name used to authenticate is compared to the following values in the certificate request submitted:

- Common Name (CN) in the request's Subject DN
- Email address in the request's subjectAltName
- DNSname in the request's subjectAltName

If the subscriber name matches one of those items, the TOE will issue a certificate matching the request.

The EST password is a one-time password. Once a subscriber has successfully enrolled using the EST user name and password, submitting a new request with the same user name and password will be rejected.

NOTE: Below settings are only available if EST has been enabled by an administrator. Only a CA Operations Staff member with 'certify' permission can manage these settings.

To view the EST users:

1. Click **Self-Service** in the Preferences section of the navigation panel.
2. Select EST User tab.
3. Specify the search criteria. Select "EST name" from the drop-down and specify a name to search, or select "All users", "All authorized users", or "All unauthorized users" from the drop-down. The result will be displayed.

To add an authorized user for basic authentication:

1. Click Add EST User.
2. Specify the user name and password in the form and click Add.

To update the password of an existing user:

1. Click the  icon for the user you wish to update.
2. Enter the new password and click **Update**.

To remove one or more authorized users, check the boxes of those you wish to delete and click **Remove Selected**. Then click **OK** in the confirmation dialog.

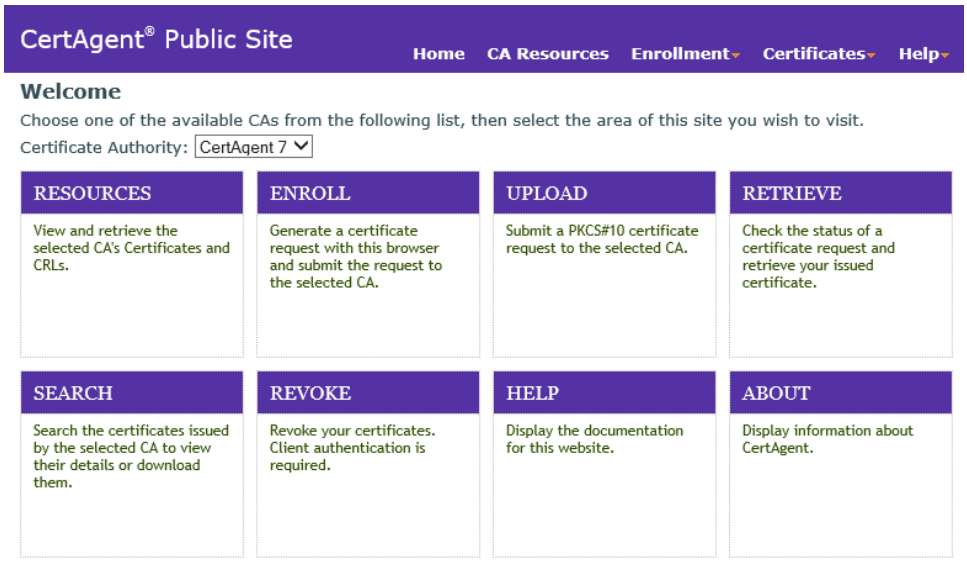
4.6 Using the Public Site

To access the CertAgent main public page for end-users, launch Firefox (or any other browser) and enter the following URL into its address bar:

```
https://<hostname/IP address>:<public port>/certagent/main.jsp
```

Be sure to replace `<hostname/IP address>` and `<public port>` with the appropriate system name or IP address and TLS port of your CertAgent webserver.

The following page will appear:



Initially, the first certificate authority in the drop-down list is displayed with its available menu items. To view the menus for a different certificate authority, select your desired certificate authority from the drop-down list.

For more information on the usage of the public site, please refer to the on-line help pages:

```
https://<hostname/IP address>:<public port>/certagent/help.html
```

4.6.1 CA Resources

To access CA-specific details such as certificates and CRLs information:

Make sure the **Certificate Authority** in which you are interested is selected on the Main page, and then click the first menu item, **Resources**.

The **CA Resources** page allow you to view the detail of the CA's certificate, and retrieve the CA's certificate and most recent CRL in various formats.

To download the CA's certificate, certificate validation path, or freshest CRL from this page:

1. Click the link for the certificate (.der), PKCS#7 file (.p7b), or CRL that you wish to download (separate links are provided to retrieve each of these items in either binary or base64-encoded format).
2. Click **Save** in the File Download dialog.
3. Select the destination folder and click **Save**.

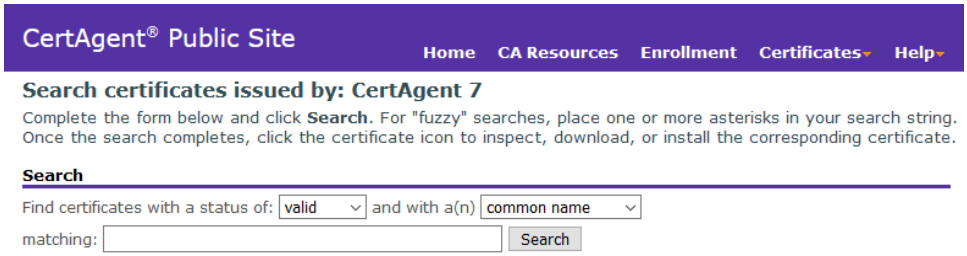
To inspect the CA's latest CRL:

1. Click the View CRL details link.
2. Click **Close** to close the CRL Information window.

4.6.2 Accessing the Certificate Database

To search for certificates issued by a particular CA:

1. If you are on the website's Main page, make sure the desired CA is selected in the drop-down list and click the **Search** menu item.
   Elsewhere in the website, simply select **Certificates, Search** in the menu bar.



2. Specify a **certificate status** (valid, revoked, expired, or any) and **search type** (common name, email address, organization, organization unit, or serial number) for your query. Then enter a **search string** (which may contain one or more asterisks '*') and click **Search**. A list of certificates matching your search criteria will be displayed.
   Clicking the icon certificate in front of a certificate in the results list will open a window containing details about that particular certificate together with several download links: These download links are described in the following table:

Download this certificate to a local binary X.509 (.der) file	The individual certificate will be saved to a local file in binary format.
Download this certificate to a local base64-encoded X.509 (.der) file	The individual certificate will be saved to a local file in base64-encoded format.
Download this certificate path to a local binary PKCS#7 (.p7b) file	The entire certificate validation path will be saved to a local file in binary format.
Download this certificate path to a local base64-encoded PKCS#7 (.p7b) file	The entire certificate validation path will be saved to a local file in base64-encoded format.

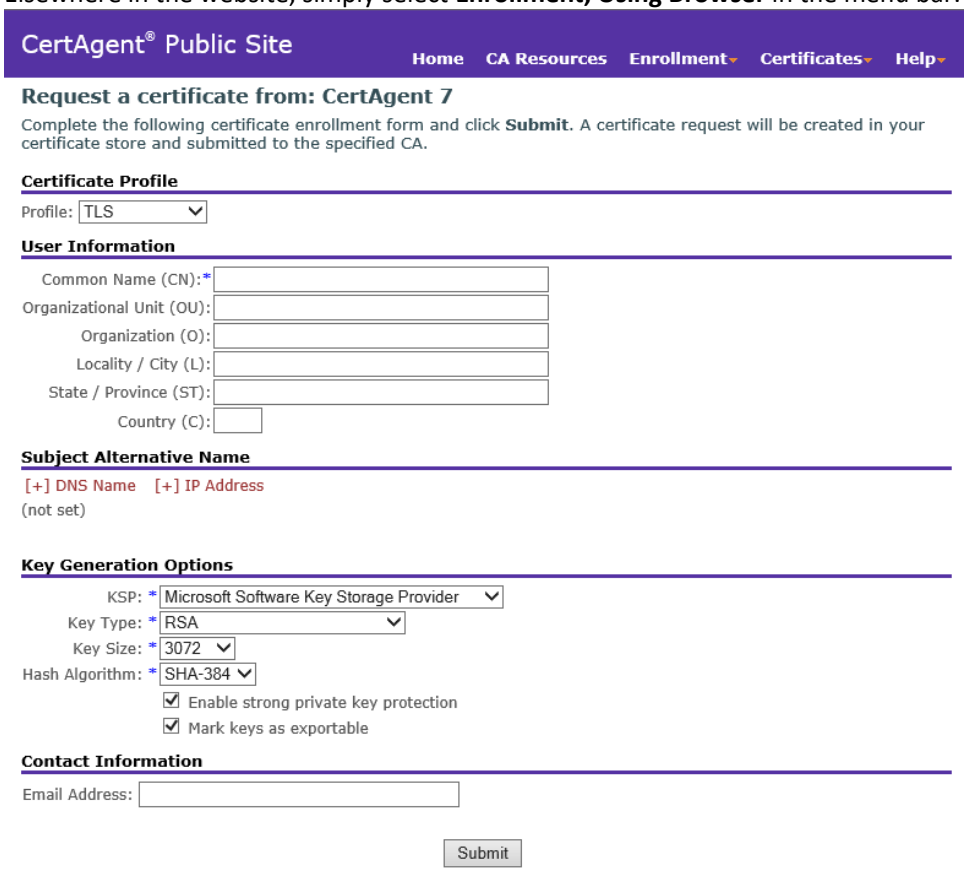
4.6.3 Browser-based Certificate Enrollment

You may use Internet Explorer to generate a public and private key pair locally and automatically submit a digitally signed certificate request containing your new public key to a specified certificate authority on the CertAgent website. Your certificate request will be added to the pending request queue for the specified certificate authority. Once they have approved your request and issued your certificate, you can return to the website to retrieve it.

To start the certificate enrollment process:

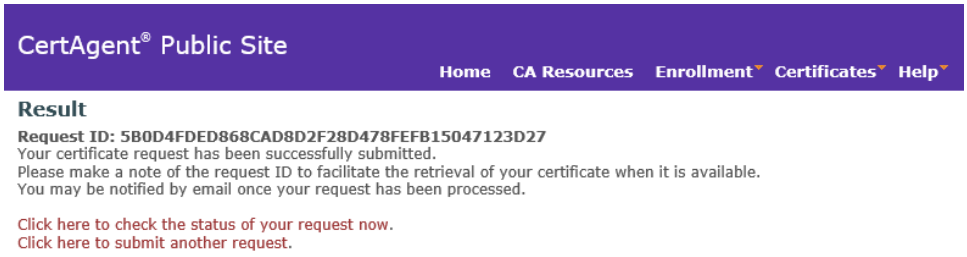
1. If you are on the website's Main page, make sure the desired CA is selected in the drop-down list and click the **Enroll** menu item.

   Elsewhere in the website, simply select **Enrollment, Using Browser** in the menu bar.



2. If the **Certificate Profile** section appears, select the desired profile.
3. Complete the form and click **Submit**.
4. If the Windows Security dialog appears, enter a key protection password and click **OK**.

   Your new key pair will be generated locally (in the specified 'security device'), and your signed certificate request will be submitted to the selected CA account. If this process is successful, the following result page will be displayed.



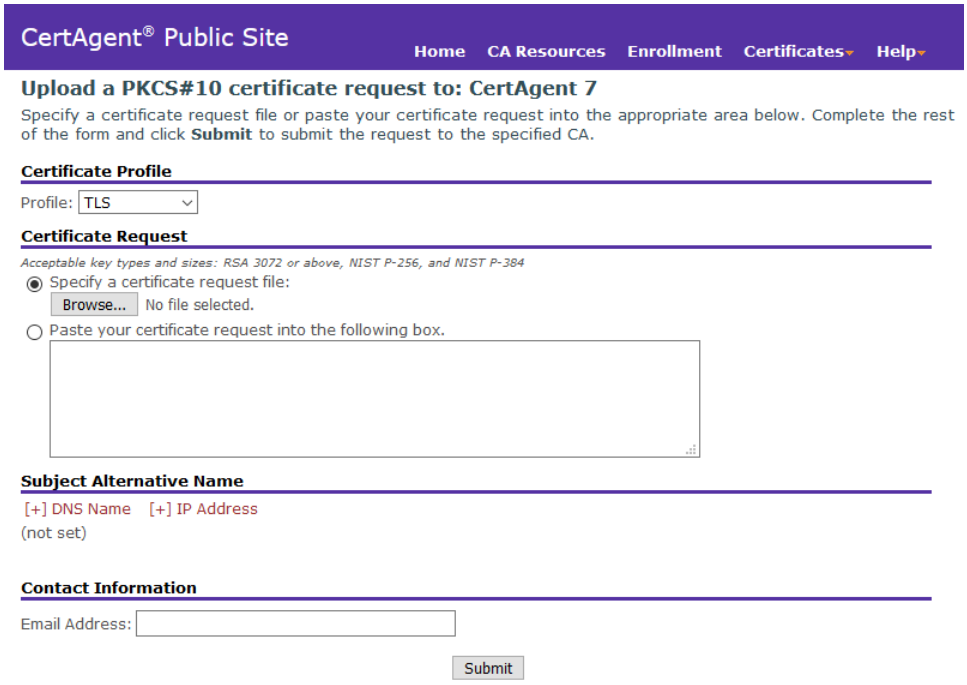
   Please make a note of your request ID as you may need it to retrieve your certificate once it has been issued. (Select the request ID by double clicking anywhere within it, press Ctrl-C to

copy it to the clipboard, then open Notepad or another editor and paste it into a note file by pressing Ctrl-V.)

4.6.4 Uploading a Certificate Request

To upload a certificate request:

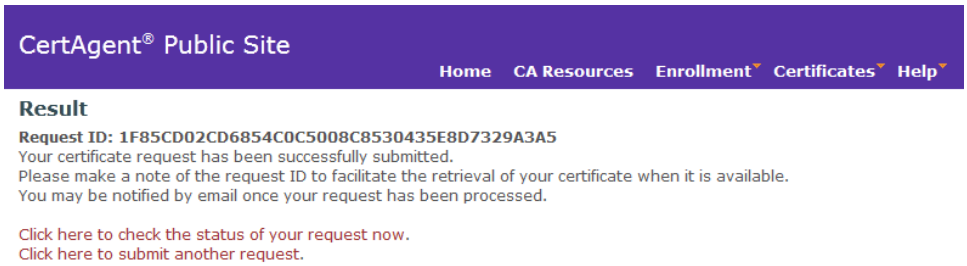
1. If you are on the website's Main page, make sure the desired CA is selected in the drop-down list and click the **Upload** menu item.
   Elsewhere in the website, simply select **Enrollment, Upload PKCS#10** in the menu bar.
   The following Upload file page will appear:



2. If the **Certificate Profile** section appears, select the desired profile.
3. Click **Browse…** to select the PKCS#10 certificate request file you wish to upload. Alternately, if your certificate request has already been copied to the clipboard, select **Paste the certificate request into the following box** and paste the base64-encoded certificate request into the provided text box.

   NOTE: The uploaded certificate request must have a valid signature, and its key type and size must be acceptable to the selected CA account; otherwise, it will automatically be rejected.
4. (Optional) If the Subject Alternative Name section appears, you may click the desired name and enter the information you wish to pass to your CA.
5. (Optional) If the comment field appears, you may enter into it any additional information you wish to pass to your CA.
6. Enter your email address so that the system can send you a notification once your request has been processed (if enabled by your CA).

7. Click **Submit** to submit your request to the selected CA.
   If the submittal process is successful, the following Result page will appear:



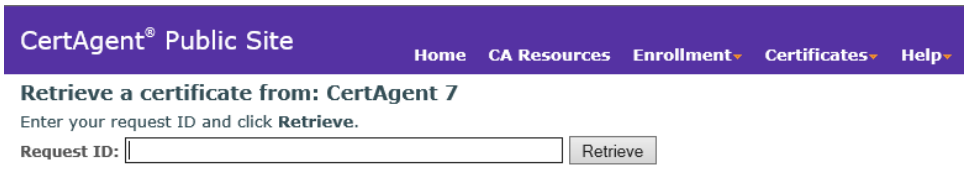
   Please make a note of your request ID as you may need it to retrieve your certificate once it has been issued. (Select the request ID by double clicking anywhere within it, press Ctrl-C to copy it to the clipboard, then open Notepad or another editor and paste it into a note file by pressing Ctrl-V.)

4.6.5 Retrieving Your Certificate

To retrieve your certificate:

1. If you are on the website's Main page, make sure the desired CA is selected in the drop-down list and click the **Retrieve** menu item.

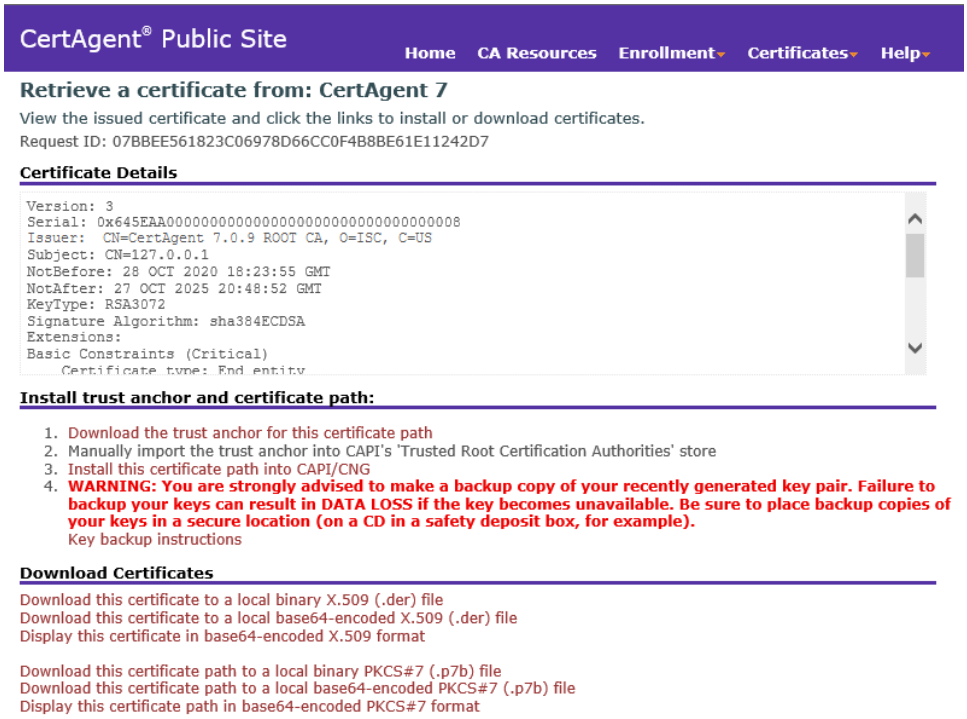
   Elsewhere in the website, simply select **Certificates, Retrieve** in the menu bar.



2. Enter the request ID that you received when you submitted your certificate request and click **Retrieve**.

   If you receive a message informing you that your request has not yet been processed, try returning to the site later. If your request was rejected, a reason should be displayed. You should consult your security officer if you continue to experience problems with the certificate enrollment process.

   If your certificate has been issued, its properties and retrieval links will be displayed.



The following table describes in detail the various links that may appear on this page:

Download the trust anchor for this certificate path	Click to download the root certificate; only displayed by Internet Explorer (installation of the root certificate into CAPI's "Trusted Root Certification Authorities" store is required before the certificate path itself can be installed)
Install this certificate path into CAPI/CNG (or into your certificate store)	Click to replace your certificate request in CAPI/CNG with your certificate and to install its validation path (for browser-based enrollment with Internet Explorer)
Key Backup instructions	Displays key backup instructions
Download this certificate to a local binary X.509 (.der) file	Click to save your certificate to a local binary file
Download this certificate to a local base64-encoded X.509 (.der) file	Click to save your certificate to a local base64-encoded file
Display this certificate in base64-encoded X.509 format	The individual certificate will be displayed in base64-encoded X.509 format.
Download this certificate path to a local binary PKCS#7 (.p7b) file	Click to save your certificate and its entire validation path to a local binary file
Download this certificate path to a local base64-encoded PKCS#7 (.p7b) file	Click to save your certificate and its entire validation path to a local base64-encoded file

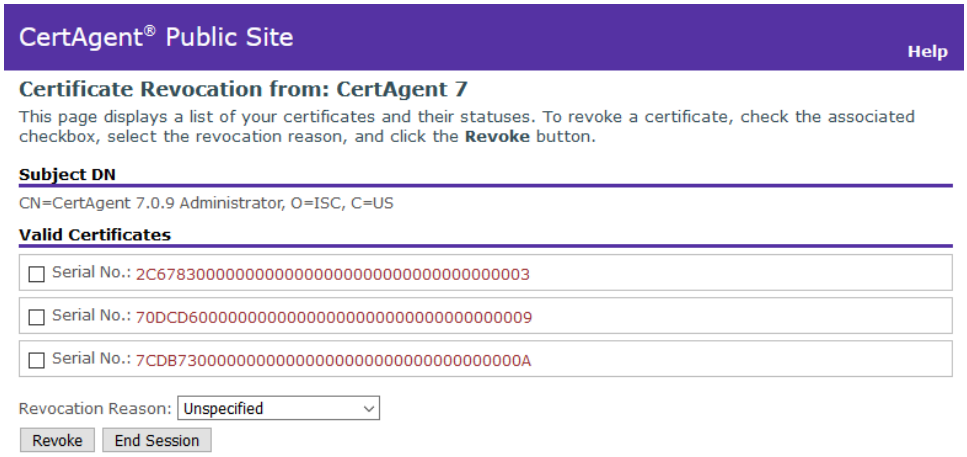
Display this certificate path in base64-encoded PKCS#7 format	The individual certificate and its chain will be displayed in base64-encoded PKCS#7 format.

4.6.6 Using Self-service Revocation

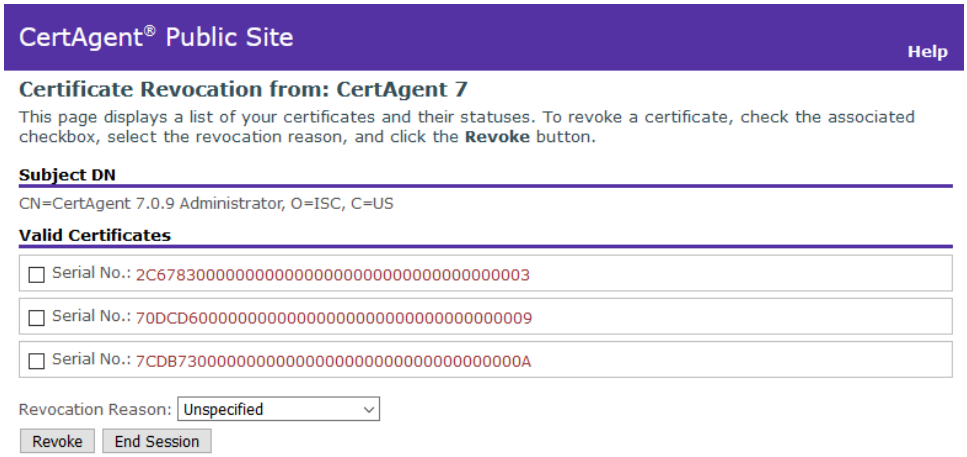
If the self-service revoking page is enabled by the CA account, users can authenticate to the page with their existing client authentication certificates issued by the same CA account.

To revoke your certificate:

1. If you are on the website's Main page, make sure the desired CA is selected in the drop-down list and click the **Revoke** menu item.
   Elsewhere in the website, simply select **Certificates, Revoke** in the menu bar.
2. Click **Authenticate**. Then, select your client certificate to authenticate to the server. Your certificate must be valid (not revoked) and issued by the selected CA.
3. If authenticated, all certificates matching the subject DN of your client certificate will be displayed.



4. To inspect a certificate, click on the desired serial number. A popup dialog with certificate information will be displayed. Click **Close** to close the dialog.
5. To revoke one or more certificates from the Valid Certificates list, check the box of each serial number you wish to revoke, select the revocation reason from the drop-down and click **Revoke**.
6. Click **OK** at the confirmation prompt to confirm.
7. The result will be displayed:



8. Click **End Session** to terminate the current session.

4.7 Using RAMI

The CertAgent Registration Authority Management Interface (RAMI):

```
URL: https://<hostname>:<TLS port>/certagentadmin/ca/rami
```

Allows a remote or automated client process (acting on behalf of an authorized user) to:

- submit a certificate request for immediate processing and obtain an issued certificate,
- revoke a certificate,
- reinstate a certificate with a status of on-hold or pending revocation,
- issue a CRL,
- retrieve the CA accounts information,
- query certificate request information,
- query certificate information,
- and retrieve an issued certificate

over a TLS-secured connection (with client authentication). Once an HTTPS connection has been established, the process simply POSTs to the server all required parameters and values for the desired operation. Response status and operation details will be returned to the client process as formatted text that may be parsed for further action by that client. In this way, an authorized *registration authority* (RA) may submit pre-screened certificate requests in an automated fashion.

Warning: Only the 'submit a certificate request', 'revoke a certificate', and 'issue a CRL' functionalities are covered by evaluation activities and described in this section.

This chapter documents the procedure to be followed by a Java-based RA. Similar consideration would apply if your application is written in a different language. A sample Java program illustrating a typical interaction with the RA Management Interface is provided in the package:

```
<ca home>/tools/RAMISample.java
```

Run the following commands as appropriate for your system to compile and run the sample program:

```
javac –classpath .:/usr/local/certagent7/lib/gson-2.8.6.jar RAMISample.java
java –classpath .:/usr/local/certagent7/lib/gson-2.8.6.jar RAMISample

javac –classpath ".;C:\Program Files\CertAgent7\lib\gson-2.8.6.jar"
RAMISample.java
java –classpath ".;C:\Program Files\CertAgent7\lib\gson-2.8.6.jar" RAMISample
```

Alternatively, RAMI requests can be submitted via the cURL command line tool on CentOS.

1. Run the following command to convert the client PKCS#12 file to PEM format:

   ```
   openssl pkcs12 -in <p12 file> -out <client pem file> -nodes
   ```

2. Run the following command to convert the trust anchor certificate to PEM format:

   ```
   openssl x509 –inform der –in <root cert> -out <root pem file>
   ```

3. Run the curl command to submit the post data specified in the data file.

   ```
   curl <url> --cert <client pem file> -v –o <out p7 file> --cacert <root
   pem file> --data-ascii @<post data file> --tlsv1.1
   ```

4.7.1 Establishing a TLS Session with Client Authentication

For anapplication to establish a TLS connection with the CertAgent RA Management Interface, the following requirements must be satisfied:

- client credentials (certificate and private key) must be available on an attached HSM, in a local PKCS#12 file, or in a Java keystore file.
- the client must possess the passwords for its own private key and the keystore in which it resides, or the HSM PIN if the credentials are stored on an HSM.
- the client's trust keystore must contain a trust anchor for the server's TLS certificate (*i.e.*, the root certificate for path validation of the server's SSL credentials).
- the server's Java trust keystore must contain the trust anchor for the user's TLS certificate.
- the client's certificate must be added to the ACL of the appropriate CA account with 'RAMI' permission.

4.7.2 Submitting a Certificate Request

4.7.2.1 Request

To submit a certificate request, and obtain a certificate, POST the following data to the RA Management Interface.

NOTE: Unsigned PKCS#10 certificate requests are acceptable if submitted via the RAMI. After issuing the certificates, these requests will be signed in CMS by the CA's private key and stored in the database.

4.7.2.1.1 Required Parameters

Parameter	Format and Description
action	"enrollKey"
ca	CA login name
request	a URL-encoded and base64-encoded PKCS#10

TABLE 22 CERTIFICATE ENROLLMENT – REQUIRED PARAMETERS

4.7.2.1.2 Optional Parameters

Parameter	Format and Description
userEmail	a list of comma-delimited e-mail addresses of the user
cert.validity.num	validity period if set, the cert.validity.unit setting is required
cert.validity.unit	validity period units: years: 1; months: 2; days: 3
cert.validity.nb	not before date number of milliseconds since 01/01/1970 00:00:00 GMT if the cert.validity.na is set and this value is not set, the issuance time will automatically be set to the not before date if set, this value cannot precede the current time
cert.validity.na	not after date number of milliseconds since 01/01/1970 00:00:00 GMT if set, the cert.validity.num setting is ignored and the specified cert.validity.nb setting will be used
response.cert.format	issued certificate format in the response if not set or set to 1, the issued certificate and chain in base64-encoded PKCS#7 format will be included in the 'base64CertChain' value of the response if set to 2, only the issued certificate in bas64-encoded X.509 format will be included in the 'base64Cert' value of the response if set to 3, both issued certificate and chain in base64-encoded PKCS#7 format and issued certificate in X.509 format will be included in the 'base54CertChain' and 'base64Cert' values respectively in the response

TABLE 23 CERTIFICATE ENROLLMENT – OPTIONAL PARAMETERS

NOTE: If the validity period is specified, the duration must be shorter than or equal to the default validity period defined in the CA account or profile. Otherwise, the request will be rejected.

4.7.2.1.3 Sample

To submit a certificate request to the CA account “testca”, post the following data:

```
action=enrollKey&ca=testca&request=MIICrzCCAZcCAQAwajELMAkGA1UEBhMCVVMxIjAgBgNV
BAoTGUluZm9ybWF0aW9uIFNlY3VyaXR5IENvcnAxDzANBgNVBAwTBlRlc3RlcjEmMCQGA1UEAxMdQ2V
ydEFnZW50IEtleSBFbnJvbGxtZW50IFRlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
DI%2BovE1NM3wzkSLDQUVEQkISQ923J1N6lY3nI2DnrYFJcYGAY8NHtMwQvv2t2TSCL5vEHbDl66t0m
i7Ka8dW2QK93USDEdE3jLdOoQ5RZb%2BoC9644%2FvJJrt%2BAs%2FQ0yU9Ba6YAvqgvedGt7jJNgFR
TbI%2Bu6Y%2Bxe49y2yC52k7GqN31eVxhspqkgOerDWfp9muYfAs6SMrT7rEkNUsNsXj6UQjKjjmBi3
He7UDrA7qADuLHwrXGqlb7hxv0u0rYpXX3NmnOFx8Uzfip0eO6%2BZToqF1uowRSazWZ43QN72yZhfN
K9fmFErXglFLWferui5joLJBHhWs%2F1%2FfZjMZtQ4xZ5AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCA
QEApRpnjFad3CR6VVzzbDkZI6osTnzpOyi4W46Ja7SO5Trf%2BEFOXchHakRVHDh4RqhClJf%2BKr%2
F9jR4sTQeEib4S%2BirTuyve3c57111xfEQug3KZ347RGa4N%2BxUQv%2BFX2cRqzUgMTI2v3dwD1as
ntsIP5d7xLkhX7QotN%2FCuwtPFWV5hdhgSzzvFrqlYgvklWyUoDt8Ch2yXORfkjhxOGXrBIFiyPrkM
eeS%2B7BzkJRiACp6affD%2BjQz5a3rDkIZE7zSOBLvIHAgeKU7X4Ir%2FLg4R7AMz6X%2Bzwq%2F31
0moPWDxJgItONZWEVzoTYECPx04%2BLQdMuln%2Bljx%2Bqy7idYyggBw2w%3D%3D
```

4.7.2.2 Response

After POSTing its request, the client process should read the response information written to the output stream of the open connection by the server.

4.7.2.2.1 Status Code and Content Type

Code	Content-Type and Description
200 (OK)	text/html Valid information was posted. Request status, detail, and other information will be returned. See the next section for details
400 (Bad Request)	text/html Invalid information was posted (e.g., invalid CA account was specified); error message will be returned

TABLE 24 CERIFICATION ENORLLMENT – RESPONSE CODE AND TYPE

4.7.2.2.2 Response Format

Parameter	Format and Description
requestStatus	A code indicating the current status of the request: 0 (success): processing the request was successful and a certificate was issued 1 (error): an error occurred while processing the request 2 (issued and error): an error occurred but the request was successfully processed and a certificate was issued
detail	The detailed information regarding the processing of the client’s request
requestID	The request ID of the certificate request
serialNo	The serial number of the issued certificate
base64CertChain	The issued certificate and chain in base-64 encoded PKCS#7 format.

TABLE 25 CERTIFICATE ENROLLMENT – RESPONSE FORMAT

4.7.2.2.3 Sample

The following are two possible responses illustrating success and failure, respectively:

```
requestStatus=0
detail=Processed request.
requestID=21CF105EF9217F7F129F16AFCA3953C64AC3BE14
serialNo=57CB8600000000000000000000000000000000001
base64CertChain=MIIKCAYJKoZIhvcNAQcCoIIJ+TCCCfUCAQExADALBgkqhkiG9w0BBwGgggndMII
DLzCCAhegAwIBAgIUKEGUcYHWbf5PaVieXCgD1JwxRfUwDQYJKoZIhvcNAQELBQAwPjELMAkGA1UEBh
MCVVMxDDAKBgNVBAoTA0lTQzEhMB8GA1UEAxMYSVNDIFNIQS0yNTYgRGVtbyBSb290IENBMCAXDTE1M
TIxMTIyMDQ1N1oYDzIwNjUxMjExMjIwNDU3WjA+MQswCQYDVQQGEwJVUzEMMAoGA1UEChMDSVNDMSEw
HwYDVQQDExhJU0MgU0hBLTI1NiBEZW1vIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggE
KAoIBAQDYo5ynqdOfCRtPaQybxAl+Ow63dqmvUGgSsLnALIiXlx6qnZu1lpP9M34p5ZOtMfQRfuktjK
j8PW7qNDsyL0cJIevCfD9j3fcYglzacldVZMFhCsfQ6eGhUa8lAPVVX3u+UtDpL9nfN8jnIKhNRphUw
lULK86KalsfqiGnR1ha2CJ+zCb0kx+E/1VvwtZ0Ck+a0XGz9SSX5cnFfly0tQe0eYZYYML4Ey5GA8Fw
5I3KIKvxu+pEa1zGLku3VeMrZC9ikRyRu9FOEMS32gb2tl68ANCSdlKjzt+xNNExKwbAfSZEUWw0ri9
rF492N0V+1Z077LeaJGp0e8VLsC0g3trLAgMBAAGjIzAhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQ
H/BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4IBAQA7v+A+NEOXFdU+SiATtdHvDyzWmaJHzMGSYCzWXnDil
Y/WTcEQnGpAFSvb31bnQa3MRyXbaYUMIyhGnftYIbukzsTM/mdxBBCqSCegpcoIuTPAYXCZ0TsVImzI
zVeXUMfktEZ4SiqnDX5I06+LHsdqTiFnNg3SGNiUYz+Z9lK9Y2oGrGt9t4Jyu0oUWnUyhrUXzDP0VaP
GYpSjblaWF3wqB2rnVXy55GxdruSkMOL/1MsKQ0O0+1b7g5RClanzRQbApvL9E3nEZw/2VXWcXBEO98
ltK0ChYDzTJUD5Xyk4FcLKaupMxTTjACi7it1b9boBJtjjFSau/B+DBN15w87fMIIDLjCCAhagAwIBA
gIUGEbcMGXeNU+yy5GHXK91P8JvDMswDQYJKoZIhvcNAQELBQAwPjELMAkGA1UEBhMCVVMxDDAKBgNV
BAoTA0lTQzEhMB8GA1UEAxMYSVNDIFNIQS0yNTYgRGVtbyBSb290IENBMCAXDTE1MTIxNDE2MDIzM1o
YDzIwNjUxMjE0MTYwMjMzWjA9MQswCQYDVQQGEwJVUzEMMAoGA1UEChMDSVNDMSAwHgYDVQQDExdJU0
MgU0hBLTI1NiBEZW1vIFN1YiBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKvPGFJoL
jn/ymwD01X0+aH4ptJHhGgCCDlHPQKcW3C58SMYJffpF+oww/6RIBIGlJtqQZxvNfKwdctDDrnaSRRE
fxPC81WjDuCPlK4wz+B6N5L969kbJ0qFP6lsRc+YTirt1e8llsC4x+Q9j6AiqaQ1HPKkPgmb8VUcSH2
bdo+2FAUqMG9mHAVotULGcmggf3mleJ4LjqasyHM88zzqWYPEFSjlLw9F4r124aFIGaYx9NpZr4/HcP
Bfsq2my31UyVOWVQEMBCog7sqWIWSGouY4yI8LpE4vj3irFPrjVy9R6RtzyuU2VznHGcX5VCIiFyZbj
+TXLWNaHut3gmgjORsCAwEAAaMjMCEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwDQYJ
KoZIhvcNAQELBQADggEBAKhvLtQOArl1u47r0JO0nNdgfLIAdvXCwtyIdQWhf56Iq1do6RbMmfe9usg
pf6L8CxOUij5CFDMKgcjRuY2P0krTmnenqoIDlqmdZuqUijfC1rSRvSBFuD1t3qg2HhSdeCkBOqIqz5
Jhap0SrLlH4AAiMLHUO+UKLgzT50fGwNb7pk8NoQ164AqGDk/0+OBbd+J6hXrlnHXouY+sYIEbgsrs8
Df3rwz+Td+MESuZ1J68E9qt+Q7gRFSW9SD5WQtnfHTPkQ+Lh/43ZehcHfJaVRWMIiln+aWpEK4qa5UV
vgtvlVSJp+ZY+REIjRHcN5wiCYCe0GicX3++HtaDjtPpfNgwggN0MIICXKADAgECAhRXy4YAAAAAAAA
AAAAAAAAAAAAAAATANBgkqhkiG9w0BAQsFADA9MQswCQYDVQQGEwJVUzEMMAoGA1UEChMDSVNDMSAwHg
YDVQQDExdJU0MgU0hBLTI1NiBEZW1vIFN1YiBDQTAeFw0xNjA4MDUxNDE3NDlaFw0xODA4MDUxNDE3N
DlaMCwxCzAJBgNVBAYMAlVTMQwwCgYDVQQKDANJU0MxDzANBgNVBAMMBlVzZXIgMTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMj6i8TU0zfDORIsNBRURCQhJD3bcnU3qVjecjYOetgUlxgYBjw
0e0zBC+/a3ZNIIvm8QdsOXrq3SaLsprx1bZAr3dRIMR0TeMt06hDlFlv6gL3rjj+8kmu34Cz9DTJT0F
rpgC+qC950a3uMk2AVFNsj67pj7F7j3LbILnaTsao3fV5XGGymqSA56sNZ+n2a5h8CzpIytPusSQ1Sw
2xePpRCMqOOYGLcd7tQOsDuoAO4sfCtcaqVvuHG/S7Stildfc2ac4XHxTN+KnR47r5lOioXW6jBFJrN
ZnjdA3vbJmF80r1+YUSteCUUtZ96u6LmOgskEeFaz/X99mMxm1DjFnkCAwEAAaN9MHsweQYDVR0jBHI
wcIAU/i2n0MKtjN4XvhVJYxbdN1Z//KChQqRAMD4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxIT
AfBgNVBAMTGElTQyBTSEEtMjU2IERlbW8gUm9vdCBDQYIUGEbcMGXeNU+yy5GHXK91P8JvDMswDQYJK
oZIhvcNAQELBQADggEBAElcdO5ZCnkA+gvEEHVI+xyulpIXMOX8AgyDEabmYkeOTIsFWwiLwhTN1w47
JlWjIfkS192HW34/9lozXV4fV8ysVPgfLvxMuZ0+N0fZsdTZy9wutI9Ba0/pG4ii2QFqFa7sluj1lBX
1zML1jW+mYUODvtvfBS3umFbBJ/GSj3x1Fw16+FnRVNtOUAHNS8HmjvwbD3mysTuHR9plYpqYp2+L88
d5uHNx+BA/5fcR52xHUATif+s5yOWT8MysD4k33zGEXyTu3wBUmcAoYUTyBe18BSX9sPJTlMoEnOT4s
S0VLWYmRjpiALvtaruvLwuVpg53J3CbYCcpMon1wbIsCUMxAA==
```

```
requestStatus=1
detail=RSA 2048 certificate request is not acceptable. Acceptable key types and
sizes: RSA 3072 or above, NIST P-256, and NIST P-384.
```

If the information posted was invalid (e.g., invalid CA account), HTTP status code 400 (bad request) and error message will be returned in the response.

4.7.3 Revoking a Certificate

4.7.3.1 Request

To revoke a certificate, POST the following information to the RA Management Interface:

Parameter	Format and Description
action	"revokeCert"
ca	CA login name
serial	Serial number of the certificate to be revoked
status	Certificate status 2: revoked 6: on hold
Reason	Reason code for revoked or on-hold status If status=2: 0: unspecified 1: key compromise 2: CA compromise 3: affiliation changed 4: superseded 5: cessation of operation 8: remove from CRL 9: privilege withdrawn 10: AA compromise If status=6: 1: none 2: call issuer 3: reject 4: pickup token

TABLE 26 CERTIFICATE REVOCATION – REQUIRED PARAMETERS

4.7.3.1.1 Sample

To revoke a certificate issued by the CA account "testca", with serial number "57CB86000000000000000000000000000000000001", and reason code Revoked – Key Compromise, post the following data:

```
action=revokeCert&ca=testca&serial=57CB860000000000000000000000000000000001&sta
tus=2&reason=1
```

4.7.3.2 Response

After POSTing its request, the client process should read the response information written to the output stream of the open connection by the server.

4.7.3.2.1 Status Code and Content Type

Code	Content-Type and Description
200 (OK)	text/html Valid information was posted. Request status and details will be returned. See the next section for details
400 (Bad Request)	text/html Invalid information was posted (e.g., invalid CA account was specified); error message will be returned

TABLE 27 CERTIFICATE REVOCATION – RESPONSE CODE AND TYPE

4.7.3.2.2 Response Format

Parameter	Format and Description
requestStatus	0 (success): certificate was revoked 1 (error): an error occurred during the processing of the revocation action 2 (revoked with error): an error occurred, but the certificate was successfully revoked anyway
detail	The detailed information regarding the processing of the client's request

TABLE 28 CERTIFICATE REVOCATION – RESPONSE FORMAT

4.7.3.2.3 Sample

The following are two possible responses illustrating success and failure, respectively:

```
requestStatus=0
detail=Certificate status changed to Revoked - Key Compromise.
```

```
requestStatus=1
detail=Certificate has already been revoked.
```

4.7.4 Issuing a CRL

4.7.4.1 Request

To issue a CRL, POST the following information to the CertAgent RAMI.

Parameter	Format and Description
action	"issueCRL"
ca	CA login name

TABLE 29 CRL ISSUANCE – REQUIRED PARAMETERS

4.7.4.1.1 Sample

To issue a CRL by the CA account "testca", post the following data:

```
action=issueCRL&ca=testca
```

4.7.4.2 Response

After POSTing its request, the client process should read the response information written to the output stream of the open connection by the server.

4.7.4.2.1 Status Code and Content Type

Code	Content-Type and Description
200 (OK)	text/html Valid information was posted. Request status, detail, and other information will be returned. See the next section for details
400 (Bad Request)	text/html Invalid information was posted (e.g., invalid CA account was specified); an error message will be returned

TABLE 30 CRL ISSUANCE – RESPONSE CODE AND TYPE

4.7.4.2.2 Response Format

Parameter	Format and Description
requestStatus	0 (success): CRL has been issued. 1 (error): Error occurred during the processing.
detail	The detailed information regarding the processing of the client's request

TABLE 31 CRL ISSUANCE – RESPONSE FORMAT

4.7.4.2.3 Sample

The following are two possible responses illustrating success and failure, respectively:

```
requestStatus=0
detail=CRL issued
```

```
requestStatus=1
detail=Invalid CA certificate: Certificate expired or not yet valid
```

4.8 Using Database Access Service

CertAgent's Database Access Service (DBAccess) can be used by remote clients to:

- retrieve the audit trail records of the admin site and CA accounts
- execute SQL Select queries (as well as Create and Drop Index commands) against the integrated certificate database on behalf of those CA accounts
- retrieve the CA account names
- retrieve the subject DN of the specified CA's current certificate
- update the contact email addresses that are associated with the certificate records

Requests are transmitted to the server over a TLS-secured connection (with client authentication) by clients who are authenticated against an ACL maintained by the administrators; authentication must succeed, or the requests are not processed.

The DBAccess library that encapsulates this functionality and exports an API that is available to authorized client processes can be found, together with sample Java code illustrating its use, in the `<ca home>/tools/dbaccess` folder.

The following table describes the method names, required permissions, ACL, and description for the supported requests:

Method Name	Permission	ACL	Description
queryCAAuditTrail	audit	CA account	Retrieve the audit trail records of the CA account
queryAdminAuditTrail	audit	Admin	Retrieve the audit trail records of the Admin site
getCADN	admin	Admin	Retrieve the subject DN of the specified CA's current certificate
getCAName	admin	Admin	Retrieve the CA account names
executeQuery	DBAccess	CA account	Query the certificate table
executeUpdate	DBAccess	CA account	Create or drop an index on the certificate table
getIndexInfo	DBAccess	CA account	Query the index information of the certificate table

replaceContactEmails	DBAccess	CA account	Replace a contact email associated with a new one for all certificate records
replaceContactEmailsBySerial	DBAccess	CA account	Replace a contact email associated with the certificate record that matches the serial number

TABLE 32 DBACCESS FUNCTIONS, PERMSSIONS AND DESCRIPTIONS

4.8.1 Developing a Java Client

To aid in the development and deployment of your Java client, you may copy the DBAccess folder (containing the Java library and sample program) from the `<ca home>/tools/dbaccess` folder on the CertAgent server to the client system. You may cut and paste the supplied sample code from your application and then link it to the DBAccess library. See the supplied API documentation for usage details.

For a Java client application to successfully use the DBAccess API, the following requirements must be satisfied:

- client credentials (certificate and private key) must be available on an attached HSM, in a local PKCS#12 file, or in a Java keystore file
- the client must possess the passwords for its own private key and the keystore in which it resides, or the HSM PIN if the credentials are stored on an HSM
- the client certificate must be installed into the ACLs with appropriate permission for which the client wishes to submit the request
- the client's Java trust keystore must contain a trust anchor for the server's TLS certificate (*i.e.*, the root certificate for path validation of the server's SSL credentials)
- the client must provide the host address and the TLS admin port for the server

4.8.2 Using the DBAccess API

A sample Java program illustrating use of the DBAccess service is provided in the package:

```
<ca home>/tools/dbaccess/DBAccessSample.java
```

The client application may be compiled using Java 1.8 or above by running the following command:

```
javac –classpath ./certagentdbaccess.jar:. DBAccessSample.java        (CentOS)
javac –classpath .\certagentdbaccess.jar;. DBAccessSample.java       (Windows)
```

To execute the client program, use the following command:

```
java -classpath ./certagentdbaccess.jar:. DBAccessSample              (CentOS)
java -classpath .\certagentdbaccess.jar;. DBAccessSample             (Windows)
```

4.8.3 Audit Table Schema

The following table describes the existing columns in the integrated CertAgent Audit table for the Admin Site and maps the database column name to the column name in the Audit Trail page.

Column Name in the Audit Trail Page	Column Name in the Database	Format and Description
Category	TYPE	Integer Type of the event: 1: credentials 2: PIN 4: ACL 8: audit 16: login 32: database 64: job 128: CA account 256: email 512: NIAP 1024: DBAccess 2048: System 4096: TLS session 8192: Dhuma
Server	SERVER	String IP address of the CertAgent system
Client	CLIENT	String IP address of the client system, CACLI, or NULL (for the events that are triggered by the system)
Date	LDATE	Timestamp Timestamp of the event
Level	LLEVEL	Integer Level of the event: 1: error 3: information
Event	EVENT	String Recorded event
ClientID	ClientID	String The identity of the client: Subject DN of an authorized user's certificate, CACLI, Startup Script, or NULL (for the events that are triggered by the system)

TABLE 33 ADMIN AUDIT TRAIL SCHEMA

The following table describes the existing columns in the integrated CertAgent Audit table for the CA account.

Column Name in the Audit Trail Page	Column Name in the Database	Format and Description
Category	TYPE	Integer 1: request 2: certificate 3: CRL 4: OCSP 5: user 6: login 7: credential 8: RAMI 9: DBAccess 10: config 11: EST 12: audit
Server	SERVER	String IP address of the CertAgent system
Client	CLIENT	String IP address of the client system, EST user name, CACLI, or NULL (for the events that are triggered by the system)
Date	LDATE	Timestamp Timestamp of the event
Level	LLEVEL	Integer Level of the event: 1: error 3: information
Event	EVENT	String Recorded event
ClientID	CLIENTID	String The identity of the client: Subject DN of an authorized user's certificate, EST user name, CACLI, or NULL (for the events that are triggered by the system)

TABLE 34 CA ACCOUNT AUDIT TABLE SCHEMA

4.9 Using CertAgent Command Line Tool (CACLI)

All system administrative tasks can be performed via the administrative and CA web interfaces. Some of these tasks can also be managed by OE Administrators via the supplied CertAgent command line program:

```
sudo <ca home>/tools/cacli/cacli.sh                    (CentOS)
<ca home>\tools\cacli\cacli.bat                        (Windows)
```

To display the usage of the command l line tool, run the following command:

```
Syntax:
-h

Example:
#> sudo ./cacli.sh -h
```

Usage will be displayed:

```
CertAgent 7.0.9.9 command line tool
Copyright(c) 1991-2023 Information Security Corp. All rights reserved.

Usage:
* Print this help, then exit
  -h

* Create CA account
  -createacct -ca <ca name> [-displayname <display name>]

* Create profile
  -createprofile -ca <ca name> -profile <profile name> [-displayname <profile
display name>]

* Assign existing credentials to a CA account
  -assign -ca <ca name> [<HSM option>] -cert <CA certificate> [-chain <CA's
chain certificates>]

* Generate key pair and assign self-signed certificate to a CA account
  -genroot -ca <ca name> -dn <dn> [<HSM option>] [-t <kypname>] [-H <hash>] [-y
<validity>] [-file <config file>]

* Generate key pair; assign certificate request to a CA account (for manual
submission of certificate request to external CA)
  -gencrq -ca <ca name> -dn <dn> [<HSM option>] -o <request output file> [-f
<output format>] [-t <kypname>] [-H <hash>]

* Generate key pair; assign certificate request to a CA account and submit to
superior CA on same system
  -gensubcrq -ca <ca name> -dn <dn> [<HSM option>] -issuer <issuer CA account>
[-email <email>] [-t <kypname>] [-H <hash>]

* Install certificate issued by a superior CA on the same system
  -install -ca <ca name>

* Install certificate issued by an external CA
  -installext -ca <ca name> -cert <issued certificate with chain>

* Display configuration settings for a CA account
  -showconf -ca <ca name> [-credential] [-rami] [-enrollment] [-est] [-
certprop] [-certext] [-crqfilter] [-revocationpolicy] [-crl] [-ocsp] [-ldap] [-
mail] [-public]

* Display configuration settings for a profile
  -showconf -profile <profile name> [-rami] [-enrollment] [-certprop] [-
certext] [-crqfilter] [-mail]

* Update preferences for an account or profile
  -updateacct (-ca <ca name> | -profile <profile name>) -file <config file>

* Display all CA accounts, or all profiles of a specified CA account
  -showacct [-ca <ca name>]

* Display the slots and labels on an HSM
  -showslots -hsmlib <library>

* Display the types of keys that can be generated
  -showkeytypes [<HSM options>]

* Display the types of hash function available for specified key type and size
  -showhash [-t <kypname>]
```

```
* Display the ACL for a CA account, profile, or Admin Site
  -showacl (-ca <ca name> | -profile <profile name> | -admin) [-acl
<permissions>]

* Add a certificate to the ACL for a CA account, profile, or Admin Site
  -addacl (-ca <ca name> | -profile <profile name> | -admin) -acl <permission>
-cert <cert file>

* Update the permissions of the ACL for a CA account, profile, or Admin Site
(lists certs and prompts for id to update)
  -updateacl (-ca <ca name> | -profile <profile name> | -admin)

* Remove a certificate from the ACL for a CA account, profile, or Admin Site
(lists certs and prompts for id to remove)
 -removeacl (-ca <ca name> | -profile <profile name> | -admin)

* Delete a particular profile
 -deleteacct -profile <profile name>

* Enable a disabled CA account
 -enableacct -ca <ca name>

* Disable an active CA account
  -disableeacct -ca <ca name>

* Import issued CRL to a CA account
  -importcrl -ca <ca name> -file <crl file>

* Import issued certificates to a CA account
  -importcert -ca <ca name> -file <cert file or directory contains cert files>

* Export certificates match the specified not before date range
  -exportcert -ca <ca name> -o <output directory> -date
   <notBeforeDate MM/dd/yyyy> [<notAfterDate MM/dd/yyyy>]
   [-fn <filename format>]

* Submit a certificate request
  -submit (-ca <ca name> | -profile <profile name>) -file <request file> [-
email <email>]

* Display trust anchors
  -showtrust
* Add a trust anchor
  -addtrust -file <cert file>

* Remove a trust anchor
  -removetrust

* Display CRLs for path validation
  -showcrl

* Add a CRL for path validation
  -addcrl -file <crl file>

* Remove a CRL for path validation
  -removecrl

* Display system information
  -getinfo

* Display unique subject DN statistics
  -statistics
```

```
HSM/PKCS#11 options (if -L is used, either -l or -s must be present):
  -L, -hsmlib <lib>      use specified vendor-supplied library for HSM
communications
  -l, -hsmlabel <label>  use specified HSM label
  -s, -hsmslot <slot>    use specified HSM slot
  -p, -hsmpin <PIN>      use specified HSM password (optional)

Options:
  -y <validity>    certificate validity period in years (default=5)
  -t <kypname>     key type and size (default=rsa-3072)
                   use -showkeytypes option to list available values
  -H <hash>        hash function (default=6 (SHA-384))
                   use -showhash option to list available values for a
                   particular key type
       4     SHA-1
       5     SHA-256
      *6     SHA-384
       7     SHA-512
       8     SHA-224
  -f <output format>    certificate request output format (default=0)
      *0   ASN.1 DER-encoded
       1   PEM-encoded
  -fn <filename format>  exported filename format (default=0)
      *0   serial number of the certificate
       1   common name of the certificate
  -email <email>        list of comma-delimited email addresses for reply
                        during certificate request submission
  -acl <permissons>     ACL permissions
   an XOR'ed combination of the following values:
       1     admin
       2     audit
       4     certify
       8     revoke
      16     RAMI
      32     DBAccess
```

Sample configuration file for can be found in `<ca home>/tools/cacli/*.txt`.

4.10 Updating the TOE

The TOE provides OE Administrators the ability to check for updates on demand via the update tool. The update tool is a command line program included with the TOE that interfaces with the TOE to verify the validity of the update's digital signature, and if valid, stops the TOE, installs the update, and restarts the TOE. At the local console, a local administrator initiates the installation of an update package using the update tool. Once initiated, the TOE verifies the digital signature on the package and will stop the process if the signature or the certificate used is not valid.

The supplied Update tool program can be used to check if an update is required, validate, and install the update package.

```
sudo <ca home>/update/update-tool.sh                    (CentOS)
<ca home>\update\update-tool.bat                        (Windows)
```

4.10.1 Displaying the Current Version

To display the TOE version:

Run the certagent script with 'version' option.

```
sudo <ca home>/certagent.sh                                    (CentOS)
<ca home>\certgent.bat                                         (Windows)
```

Example:

```
C:\Program Files\CertAgent7> certagent.bat version
CertAgent version: 7.0.9
JNI version: 7.0.9
SA version: 7.7.2.0
CDK version: 8.0.0.8; FIPS mode enabled

CertAgent was developed by:
  Information Security Corporation
  1011 W. Lake Street, Suite 425
  Oak Park, IL 60301
  Phone: 708-445-1704
  Fax: 708-445-9705

For up-to-date product information visit:
http://www.infoseccorp.com/support/ca/contents.htm
To contact technical support email tech@infoseccorp.com
```

4.10.2 Checking for Update

To check for an update:

1. Run the update tool with '-check' option.
2. It will display the current version and connect to ISC's web page (https://www.infoseccorp.com/inc/products.xml) for the latest version number and released date

   Example:

```
C:\Program Files\CertAgent7\update> update-tool -check
CertAgent 7.0.9 Update Tool
Copyright(c) 1991-2020 Information Security Corp. All rights reserved.

****************************************
Checking for update...
****************************************
Installed version: 7.0.9
Your version is up-to-date.
```

4.10.3 Obtaining the Update Package

TOE update packages are delivered in a zipped archive via ISC's website. If a newer version is available, login to the ISC's website and download the update package.

4.10.4 Verifying the Update Package

To validate the update package:

1. Use the following command to verify the signed update package:

```
<ca home>/update/update-tool.sh -verify <p7m file>              (CentOS)
<ca home>\update\update-tool.bat -verify <p7m file>            (Windows)
```

The TOE will verify the signature, obtain the signer certificate information, perform a path validation checking, and verify the version from the package. The result will be recorded in the audit trail. If the certificate is valid with proper extensions (code signing purpose in extend key usage and digital signature purpose in key usage) and its root certificate is in the trust anchor database, the signer certificate information and package information will be displayed. If the package or the signer certificate is invalid, the error will be displayed.

Example (Verify an update package 7.0.9 from a 7.0.8 installation):

```
C:\Program Files\CertAgent7\update> update-tool -verify certagent.7.0.9-
update.win.x64.p7m
CertAgent 7.0.8 Update Tool
Copyright(c) 1991-2020 Information Security Corp. All rights reserved.

*****************************************
Verifying the update package...
*****************************************

* Verifying the signature of the package...
Signer certificate:
  Serial: 11E022A8A5E3F378C7C8AD97597D69912358C523
  Issuer: CN=Information Security Corporation CA 5, L=Oak Park, O=ISC,
ST=IL, C=US
  Subject: CN=Information Security Corporation Code Signing Certificate,
L=Oak Park, O=ISC, ST=IL, C=US
  NotBefore: 05/29/17 19:00:00 CDT
  NotAfter: 05/29/37 19:00:00 CDT
Signature verified.

* Verifying signer certificate...
Verified signer certificate with path validation

* Verifying package information...
Version: 7.0.9
Verified.

Update package verified.
EXIT
```

If same or older version of update package is specified, a warning message will appear in the Verify package information section.

Example:

```
* Verifying package information...
Version: 7.0.9
Verified.
Warning: Version 7.0.9 has already been installed.
```

4.10.5 Installing the Update

To install the update:

1. Once the signed package has been verified, run the following command to install the update package:

```
<ca home>/update/update-tool.sh -install <p7m file>              (CentOS)
<ca home>\update\update-tool.bat -install <p7m file>            (Windows)
```

The TOE will verify the package as described in the previous section. Program files will be extracted.

Example (Install an update package 7.0.9 from a 7.0.8 installation):

```
C:\Program Files\CertAgent7\update> update-tool -install certagent.7.0.
9-update.win.x64.p7m
CertAgent 7.0.8 Update Tool
Copyright(c) 1991-2020 Information Security Corp. All rights reserved.

*****************************************
Verifying and Installing the update package...
*****************************************
* Verifying update package; please wait...

* Verifying the signature of the package...
Signer certificate:
  Serial: 11E022A8A5E3F378C7C8AD97597D69912358C523
  Issuer: CN=Information Security Corporation CA 5, L=Oak Park, O=ISC,
ST=IL, C=US
  Subject: CN=Information Security Corporation Code Signing Certificate,
L=Oak Park, O=ISC, ST=IL, C=US
  NotBefore: 05/29/17 19:00:00 CDT
  NotAfter: 05/29/37 19:00:00 CDT
Signature verified.

* Verifying signer certificate...
Verified signer certificate with path validation

* Verifying package information...
Version: 7.0.9
Verified.

* Extracting program files; please wait...
Files extracted.
```

2. Review the package and signer information. Enter **yes** when prompted:

```
Update package verified.
Do you want to install the update now? (yes/no): yes
```

3. The update script in the package will be executed. The update process will begin. The result will be recorded to the server's audit trail and saved to a local file.

```
* Stopping CertAgent service...
Stopping CertAgent Server Controller.
CertAgent Server Controller stopped.

* Backing Up CertAgent files...
Backing up CertAgent program directories to C:\Program
Files\CertAgenet7\update\backup_v708...

* Updating CertAgent files...
<list of files>

* Updating Tomcat files...
<list of files>

* Starting CertAgent service...CertAgent Server Controller
started.CertAgent 7.0.9 update completed.

Result saved to C:\Program Files\CertAgent7\update\update-7.0.9-
<YYYY.MM.DD_hh.mm.ss>.log

Please run the 'certagent.bat setpin' command to set the system PIN.
EXIT
```

4.11 Replacing TLS Credentials

The TLS and administrator credentials generated by the installer should be considered temporary and only used to facilitate initial system setup. Once CertAgent is configured with operational CA accounts, these credentials should be replaced with properly issued credentials before making the system operational.

4.11.1 Creating a Profile to Issue TLS Certificates

A profile to issue TLS certificates with key usage (digital signature and key encipherment), extended key usage (server authentication, client authentication, and CMC Registration Authority), and subject alternative name (with accept IP address or DNS name values from the public enrollment page) extensions is needed. Login to a CA account as CA Operations Staff. Then, follow the steps in section *4.5.7.3 Managing Certificate Profiles* and *4.5.7.4 Managing Certificate Issuance* to create a new profile and configure the default extension settings. The sample profile (TLS) configuration can be found in the default ca7 account.

4.11.2 Generating a New TLS Credential on a Luna USB HSM

1. Login to the Operating System as OE Administrator.
2. Locate the cmu tool from the following directory:

   `/usr/safenet/lunaclient/bin` (CentOS)

```
C:\Program Files\SafeNet\LunaClient                    (Windows)
```

NOTE: Each cmu command requires selecting a token and entering the password. Select the user partition (e.g., slot 0) and enter its password when prompted.

3. Run the following command to list the objects on the HSM:

```
cmu list -display=handle,class,keyType,label,id
```

4. Review the label and id values of the existing objects. Pick a new label (e.g., newtls) and a hexadecimal integer value (e.g., aa) for the new key pair. Then, run the following command to generate a new RSA-3072 key pair and assign the label and id to it:

```
cmu generatekeypair -modulusBits 3072 -publicExponent 65537 -label
newtls -id aa -sign=T -verify=T
```

5. Enter '2' when prompted for the RSA mechanism type:

```
Select RSA Mechanism Type –
[1] PKCS [2] FIPS 186-3 Only Primes [3] FIPS 186-3 Auxiliary Primes : 2
```

6. Run the following command to list the new key pair and retrieve the public key and private key handles:

```
cmu list -display=handle,class,keyType,label,id -label=newtls
```

Sample result:

```
handle=74       class=publicKey  label=newtls   id=aa
handle=75       class=privateKey label=newtls   id=aa
```

7. Run the following command to generate a certificate request:

```
cmu requestcertificate –publichandle=<handle#> -privatehandle=<handle#>
-C=US –O=<organization> -CN=<domain name/IP address> -outputFile=<output
file name>
```

Specify the public and private handles, organization, domain name, and output file name as appropriate for your configuration.

Sample command to generate a certificate request with the subject: CN=192.168.0.82, O=ISC, C=US:

```
cmu requestcertificate –publichandle=74 -privatehandle=75 -C=US –O=ISC -
CN=192.168.0.82 -outputFile=request.crq
```

4.11.3 Submitting the Certificate Request to a CA account:

1. Login to the Operating System as OE Administrator.
2. Launch Firefox and go to the Main page of the Public site.
3. Select the desired CA account and select **Upload**.
4. Select the profile for server certificates.

5. Click **Browse…** to select the PKCS#10 certificate request file you wish to upload.
6. Complete the rest of the form and click **Submit**.

   The result message will appear. Make a note of your request ID as you may need it to retrieve your certificate once it has been issued.

4.11.4 Issuing the Server Certificate

Once the request has been submitted, a CA Operations Staff member can issue the TLS certificate via the CA Account site. For details, see section *4.5.4.3 Issuing Certificates*.

4.11.5 Retrieving the Server Certificate

1. Login to the Operating System as OE Administrator.
2. Launch Firefox and go to the Main page of the Public site.
3. Select the desired CA account and select **Retrieve**.
4. Enter the request ID you received when you submitted your certificate request and click **Retrieve**.
5. Click the 'Download this certificate path to a local binary X.509 (.der) file' link.

4.11.6 Importing the Server Certificate and Chain into a Thales Luna USB HSM

To import the server certificate:

1. Login to the Operating System as OE Administrator.
2. Run the following command to import the certificate. Specify the label and certificate file as appropriate for your configuration.

```
cmu import -label newtls -inputFile=tls.der
```

3. Run the following command to verify the certificate has been imported and retrieve the handle value for the certificate.

```
cmu list -display=handle,class,label,id -label=newtls
```

   Sample result:

```
handle=74       class=publicKey   label=newtls   id=aa
handle=32       class=certificate label=newtls   id=
handle=75       class=privateKey  label=newtls   id=aa
```

4. Run the following command to set the id attribute of the certificate:

```
cmu setattribute
```

   Enter the handle value of the certificate when prompted:

```
Enter handler (or 0 for exit) : 32
```

   Enter the attribute: 'id=aa' when prompted:

```
Enter attribute (attribute=value) : id=aa
```

If your TLS certificate is issued by an intermediate CA, all intermediate CA certificates and optionally the root certificate must be imported into the HSM. During the TLS handshake, Tomcat will send the TLS certificate and its chain to the client for certificate validation.

To import an issuer certificate, run the following command. Specify the label and certificate file as appropriate for your configuration.

```
cmu import -label <label> -inputFile=<ca cert file>
```

4.11.7 Updating the CertAgent Configuration File

If the subject DN of the new TLS certificate is not the same as the current one, update the CertAgent configuration to use the new TLS credential.

1. Login to the Operating System as OE Administrator.
2. Open the following CertAgent configuration file in an editor:

   `<ca home>/acalashim/acalashim.xml`
3. Locate the HSM_CERT_FILTER value and replace it with the subject DN of the new TLS certificate.

   ```
   ...
   HSM_CERT_FILTER=CN=192.168.0.82, O=ISC, C=US
   ...
   ```

   NOTE: If the DN contains a state or province name component, use ST (e.g., ST=IL) instead of S (e.g., S=IL).
4. Save the file and close your editor

4.11.8 Deleting the Current TLS Credential

If the subject DN of the new TLS certificate is the same as the current one, the current TLS credential must be deleted.

1. Login to the Operating System as OE Administrator.
2. Stop the CertAgent service.
3. Run the following command to list the objects on the HSM:

   ```
   cmu list -display=handle,class,label,id,serialNumber
   ```
4. Locate the label of the certificate entry with the serial number that matches your current TLS certificate. Locate all the handle values that match the label. For each handle, run the following command to delete the object:

```
cmu delete -handle=<handle#>
```

4.11.9 Restarting the CertAgent Service

Once the new TLS credential has been installed and configured, restart the CertAgent service and set the PIN.

4.12 Retrieving System Information and CA Resources

CertAgent's `getinfo.jsp` page:

```
http[s]://<hostname>:<port>/certagent/getinfo.jsp
```

NOTE: The page can be access via the default port for the public site (HTTPS without client authentication) or an HTTP port (if configured manually).

Allows a remote or automated client process to:

- retrieve CertAgent version, system time, and version information.
- retrieve CA certificate and optional chain.
- retrieve a CRL.

4.12.1 Retrieving CertAgent Version and System Information

4.12.1.1 Request

To retrieve the CertAgent version and system information, submit a GET or POST request to the following URL:

```
http[s]://<hostname>:<port>/certagent/getinfo.jsp?type=SYSTEM
```

4.12.1.2 Response

An HTTP status code 200 (OK), a JSON object containing the following information of Content-Type application/json will be returned.

Parameter	Format and Description
CertAgent	String Version number of CertAgent
CDK	String Version number of ISC CDK library
SA	String Version number of ISC SA library

JNI	String Version number of JNI library
FIPS	Boolean True fi the ISC CDK library is in FIPS mode
OS	String Operating system CertAgent is running on: “Windows” or “Linux”
time	String Current date and time of the system in mm/dd/yy hh:mm:ss zZ format Example: 09/01/20 09:58:49 CDT-0600
NIAP	Boolean True if CertAgent is operating in NIAP mode
maintenance	Boolean True if CertAgent is operating in maintenance mode
error	String Optional; Error message if CDK is in error state

TABLE 35 SYSTEM INFORMATION PARAEMTERS AND DESCRIPTIONS

4.12.1.3 Sample

```
{"CertAgent":"7.0.9.9","JNI":"7.0.9.3","SA":"7.7.2.4","CDK":"8.0.0.8","FIPS":tr
ue,"OS":"Windows","time":"04/06/2023 09:58:49 CDT-
0500","NIAP":false,"maintenance":false}
```

4.12.2 Retrieving CA Resources

4.12.2.1 Request

To retrieve the CA’s certificates or CRL, submit a GET or POST request to the following URL:

```
http[s]://<hostname>:<port>/certagent/getinfo.jsp?ca=<ca name>&type=<type>
```

Parameter	Format and Description
ca	CA login name
type	text/html “CA_BIN” | “CA_PEM” | “CA_P7_BIN” | “CA_P7_PEM” | “CRL_BIN” | “CRL_PEM”

TABLE 36 CA RESOURCES PARAMETERS AND DESCRIPTIONS

4.12.2.2 Response

Status Code and Content Type:

Code	Content Type and Description
200 (OK)	Valid information was posted. See the next section for details
400 (Bad Request)	text/html Invalid information was posted (e.g., invalid CA account was specified); error message will be returned

TABLE 37 CA RESOURCES RESPONSE CODES AND DESCRIPTIONS

Response Format:

Type Value	Format and Description
CA_BIN	application/pkix-cert CA certificate in binary format
CA_PEM	application/pkix-cert CA certificate in PEM-encoded format
CA_P7_BIN	application/x-pkcs7-mime CA certificate and its chain in binary PKCS#7 format
CA_P7_PEM	application/x-pkcs7-mime CA certificate and its chin in PEM-encoded PKCS#7 format
CRL_BIN	application/pkix-crl CRL in binary format
CRL_PEM	application/pkix-crl CRL in PEM-encoded format

TABLE 38 CA RESOURCES RESPONSE FORMATS AND DESCRIPTIONS

5. Guidance

This section provides the instructions to configure CertAgent for the tests to be run for all Security Functional Requirements (SFRs) that are claimed for the TOE.

5.1 Prerequisite

5.1.1 Entering System PIN

Upon installation, or each time the TOE is restarted, an administrator must enter the PIN of the HSM in which the system credential resided. For details, see section *4.2 Entering System PIN.*

5.1.2 Importing Privileged User Credentials into Firefox

Privileged user credentials have been created during the installation and they must be installed in Firefox before accessing the TOE's Admin and CA Account Sites. For details, see section *4.3 Importing Privileged User Credentials into Firefox.*

5.1.3 Operating the TOE in NIAP Compliant Mode

In order for the TOE to operate in NIAP compliant mode, all the settings in the NIAP Conformance Setting page must be enabled. Upon installation, all settings except the Access Banner are enabled. Follow the steps in section *4.4.2 Managing NIAP Conformance Settings* to launch the NIAP Conformance page and section *4.4.2.8 Access Banner* to configure the access banner option.

5.1.4 Configuring RAMI

The TOE supports RA Management Interface (RAMI) to allow authorized RA to enroll certificates, revoke certificates, and issue CRLs. By default, this interface is disabled. To enable this service, follow the steps in section *4.5.7.2 RAMI (Registration Authority Management Interface)* and enable the following options:

- Allow certificate enrollment
- Allow CRL issuance
- Allow certificate revocation and reinstatement

5.1.5 Configuring OCSP Responder Service

The TOE supports OCSP responder service for issuers hosting by the TOE and external issuers. The OCSP service is disabled by default. To enable this service for the issuers (e.g., ca7 account) hosting by the TOE, follow the steps in section *4.5.7.6 Managing OCSP Responder Settings*. To enable this service for external issuers, see section *4.4.10 Managing Dhuma Accounts.*

5.1.6 Configuring EST

The TOE supports EST's simple enrollment, which is disabled by default.

To enable this service, follow the steps in section *4.5.7.1.3 EST (Enrollment over Secure Transport).* EST service allows subscribers with existing credentials and a special RA to enroll via the EST using client authentication interface.

For the subscribers without valid credentials for client authentication, a CA Operations Staff member must add the common name of the subscriber to the EST list and create an EST password. Follow the steps in section *4.5.7.9.2 EST (Enrollment over Secure Transport) Users* to add subscribers to the list.

5.1.7 Configuring Self-Service Certificate Revocation

The TOE supports subscriber self-service certificate revocation, which is disabled by default. To enable this option, follow the steps in section 4.5.7.9.1 Certificate Revocation.

5.1.8 Configuring Audit Setting in CentOS

By default, the time changed event doesn't record in the system log in CentOS.

To configure the audit service:

1. Login to CentOS as root.
2. Run the following command to check the status of the `auditd` service:

```
service auditd status
```

3. If it is not running, run the following command to start the service:

```
service auditd start
```

4. Open the audit configuration file in an editor:
   `/etc/audit/rules.d/audit.rules`
5. Append the following configurations to the end of the file.

```
-a exit,always -S adjtimex -S settimeofday -S clock_settime -k time-
change
-w /etc/localtime -p wa -k time-change
```

6. Save the file and close your editor.
7. Audit files are stored in `/var/log/audit`. By default, only the root can access them. To permit the auditor group to read the audit log:
   a. Open the audit configuration file in an editor:
      `/etc/audit/auditd.conf`
   b. Change the configuration "`log_group = root`" to "`log_group = ca_audit`" where ca_audit is the auditor group created for OE Auditors.
   c. Save the file and close your editor.

8. To grant the auditor group the permission to access the folder where the audit files are stored, run the following command:

```
chown root:ca_audit /var/log/audit
```

9. Restart the auditd service by running the following command:

```
service auditd restart
```

When time changed, an event will be recorded to the audit file (`/etc/audit/audit.log`). This file will have a group read permission and set to the ca_audit group. These type of events can be identified the key field (key="time-change") where time-change is the name defined in the -k option in the audit configuration file.

5.2 Security Audit (FAU)

5.2.1 Audit Trails

The TOE both implements audit functionality and interface with the Operational Environment to generate audit records for all PP required auditable events. The auditable events are listed in the below table and each is labeled with the responsible component.

Requirement	Auditable Events	Additional Audit Record Contents	Retention	Responsible Component
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None.	Normal	TOE
FCS_CKM.1	All occurrences of non-ephemeral and [no other] key generation for TOE related functions.	Success: public key generated	Normal	TOE
FCS_CKM.2	All occurrences of non-ephemeral and [no other] key generation for TOE related functions.	Success: key established	Normal	TOE
FCS_CKM_EXT.4	Failure of the key destruction process for TOE related keys.	Identity of object or entity being cleared.	n/a	n/a
FCS_CKM_EXT.5	Detection of integrity violation for stored TSF data.	None.	Normal	TOE
FCS_COP.1(2)	All occurrences of signature generation using a CA signing key. Failure in signature generation	Name/identifier of object being signed Identifier of key used for signing. None	Extended Normal	TOE

FCS_HTTPS_EXT.1	Failure to establish a HTTPS session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Normal	TOE
FCS_TLSS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. None	Normal	TOE
FCS_TLSS_EXT.2	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. None	Normal	TOE
FDP_CER_EXT.1	Certificate generation.	Success: [certificate object identified]	Extended	TOE
FDP_CER_EXT.2	Linking of certificate to certificate request.	Success: [certificate object identifier], [link to certificate request object identifier] Failure: Reason for failure, [link to certificate request object identifier].	Extended	TOE
FDP_CER_EXT.3	Failed certificate approvals.	Reason for failure, [link to certificate request object identifier].	Normal	TOE
FDP_STG_EXT.1	Changes to the trusted public keys and certificates relevant to TOE functions, including additions and deletions	The public key and all context information associated with the key.	Normal	TOE
FDP_CRL_EXT.1	Failure to generate a CRL.	None.	Normal	TOE
FDP_OCSPG_EXT.1	Failure to generate certificate status information.	None.	Extended	TOE
FIA_X509_EXT.1	Failed certificate validations.	None.	Normal	TOE
FIA_X509_EXT.2	Failed authentications.	None.	Normal	TOE
FIA_UAU_EXT.1	All uses of the authentication mechanism for access to TOE related functions.	Origin of the attempt (e.g., IP address).	Normal	TOE
FIA_UIA_EXT.1	All use of the identification and authentication mechanism used for TOE	Provided user identity. Origin of the attempt (e.g., IP address).	Normal	TOE

	related roles.			
FIA_ESTS_EXT.1	EST requests (generated or received) containing certificate request or revocation requests EST responses issued.	Identifiers for all entities authenticating the request, including the entity providing client authentication for the EST transport (if any). The submitted request. Any signed response.	Extended	TOE
FMT_SMR.2	Modifications to the group of users that are part of a role.	Modifications to the group of users that are part of a role.	Extended	TOE
FPT_FLS.1	Invocation of failures under this requirement.	Indication that the TSF has failed with the type of failure that occurred.	Normal	TOE
FPT_KST_EXT.2	All unauthorized attempts to use TOE secret and private keys.	Identifier of user or process that attempted access.	Normal	TOE
FPT_RCV.1	The fact that a failure or service discontinuity occurred; resumption of the regular operation	The type of failure or service discontinuity	Extended	TOE
FPT_STM.1	Changes to the time.	The old and new values for the time.	Normal	Operating system
FPT_TUD_EXT.1	Initiation of update.	Version number	Extended	TOE
FPT_TST_EXT.2	Execution of this set of TSF integrity tests. Detected integrity violations.	For integrity violations, the identity of the object that caused the integrity violation.	Normal	TOE
FTA_SSL.4	The termination of an interactive session.	None.	Normal	TOE
FTA_SSL.3	The termination of a remote session by the session termination mechanism.	None.	Normal	TOE
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	Normal	TOE
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment	Normal	TOE

	Failure of the trusted channel functions.	attempt.		

TABLE 39 TOE AUDITABLE EVENT TYPES AND STORAGE LOCATIONS

5.2.2 FAU_GEN.1 Audit Data Generation

5.2.2.1 FAU_GEN.1.1

The TOE audits the startup of its audit functions and the use of all the administrative functions required by the FMT SFRs. The TOE also generates audit records for all the auditable events identified in Table 39 above. For each auditable event, the date, time, type, subject identity (usually the DN from the certificate used to authenticate), and outcome of the event is recorded. Additional data is collected as listed in Table 39. The TOE does not include different levels of audit. All audit data is generated by the TOE in response to actions taken by the TOE itself, privileged users, subscribers, or relying parties.

The TOE relies on the environmental Operating System's audit facility to generate audit entries for services that the Operating System provides. The Operating System supplies time services to the TOE. The Operating System's own audit capabilities audit changes to the system clock (FPT_STM.1). On the Windows platform, no specific configurations are needed for the OS generated audit event. Audit records can be viewed via the Windows Event Viewer. On the CentOS platform, a configuration is required. For details, see section *5.1.8 Configuring Audit Setting in CentOS*.

5.2.2.2 FAU_GEN.1.2

The TOE maintains its audit trail in an external database installed on its underlying platform. The audit trail comprises the audit records stored in database tables on the host platform and local server log file that records the TOE startup and shut down processes and fatal errors.

Auditors can search and view the audit data stored in the database table from the Admin and CA Site. For details, see sections *4.4.3 Searching the Audit Trail* and *4.5.2 Searching the Audit Trail*.

The TOE also provides the DBAccess interface which can be used to retrieve audit data from the database tables; only Auditors can retrieve the audit data using this interface. For details, see section *4.8 Using Database Access Service*.

The local server log file is stored in the CertAgent directory and is accessible only via the local console. Only Administrators on the OS platform can access the server log file.

The Operating Systems maintain their own event log systems.

5.2.2.2.1 Audit Tables in Database

There is one administrative audit log table in the database (Admin Audit table named CA_ADMIN_AUDIT), each issuer (CA account) has its own audit log table (CA Audit table named CA_AUDIT_<ca ID>) in the database.

For each auditable event, the date, time, type, subject identity (usually the DN from the certificate used to authenticate), and outcome of the event is recorded in the Audit Tables. The TOE audits the startup of its audit functions, and all administrative actions are audited.

The TOE stores the audit records for the following auditable events in the database tables: login and all use of the identification and authentication mechanisms, certificate validation and related operations, management of TSF functions and TSF data, Cryptographic Operations, establish trust paths, EST enrollment, and certificate and CRL issuance.

Auditors can search and view the audit trail records from the Admin and CA account sites.

The description of each available field, the format of the field, and data displayed in the Audit Trail page of the Admin Site are given in the following:

Field	Format and Description
Date	Timestamp of the event in string Format: MM/DD/YY HH:MM:SS ZZZ e.g. 08/17/20 11:16:17 CDT
Server	IP address of the CertAgent system in string e.g. 169.254.9.223
Client	IP address of the client system in string; [system] if the event triggered by the system
Category	Type of the event in string: ACL Audit CA account Credential Database DBAccess Email Job Login NIAP PIN System TLS session Dhuma
Level	Level of the event in string: INFO or ERROR
Client ID	The identity of the client in string: Subject DN of an authorized user's certificate, CACLI, Installer, Startup Script, Update Tool, or (n/a) (for the events that are triggered by the system)

Event	Recorded events in string

TABLE 40 ADMIN AUDIT TRAIL FIELD AND DESCRIPTION

The description of each available field, the format of the field, and data displayed in the Audit Trail page of the CA Site are given in the following:

Field	Format and Description
Date	Timestamp of the event in string Format: MM/DD/YY HH:MM:SS ZZZ e.g. 08/17/20 11:16:17 CDT
Server	IP address of the CertAgent system in string e.g. 169.254.9.223
Client	IP address of the client system in string; [system] if the event triggered by the system
Category	Type of the event in string: request certificate CRL OCSP user login credential RAMI DBAccess configuration EST audit
Level	Level of the event in string: INFO or ERROR
Client ID	The identity of the client in string: Subject DN of an authorized user's certificate, EST user name, CACLI, or (n/a) (for the events that are triggered by the system)
Profile	Logged in CA account or profile ID in string
Event	Recorded events in string

TABLE 41 CA ACCOUNT AUDIT TRAIL FIELD AND DESCRIPTION

The following table describes the mapping between the PP required audit fields and the fields in the Audit Trail page:

PP Required Field	Audit Trail Field
Date and time of the event	Date
Type of event	Category
Subject identity	Client and Client ID
Outcome (success or failure) of the event	Event
Additional audit record contents	Event

TABLE 42 AUIDT TRAIL FIELD MAPPING

The TOE audits the SFRs with the associated database table name and sample logs in the following table.

NOTE: In each sample log, only Date, Category, Client, Client ID, and Event fields are included. The Server and Level fields are omitted, and they should set to the following values:

- Server: <IP address of the TOE system>
- Level: INFO or ERROR (for failed events)

NOTE: The required additional audit record contents for each SFR in the sample event are underlined.

Requirement	Table Name (Description)	Sample Log
FAU_GEN.1.1	Admin table (Start-up of the TSF audit functions)	Date: 09/01/20 09:08:04 CDT Client: [system] Category: audit Client ID: (n/a) Event: Audit function started
FAU_SEL.1	Admin table	Date: 09/01/20 09:28:04 CDT Client: 10.1.10.194 Category: audit Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Updated audit trail configuration: CertAgent: (TLS session: [disabled] -> [enabled])
FCS_CKM.1	Admin table (Generated TLS server credential)	Date: 09/01/20 09:04:54 CDT Client: 127.0.0.1 Category: system Client ID: Installer Event: Generated key pair and certificate request on HSM for TLS; Request: (Subject: CN=192.168.144.161, O=ISC, C=US; Base64-encoded: MIIDejCCAeICAQAwNTELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEYMBYGA1UEAxMPMTkyLjE2OC4xNDQuMTYxMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEArLGKQ/36L0P0akWUJh5+cSWKeuH/H/efqMT0V2jDVqyHBmUy/P3LyZwz3tOmtpzvShj4ALTFbNNmdLtd0mp0E7+3QCcjqxIIRdW3QB2u1IJXOIr076qMrU0iDcwreBSpL2qiUWH48wcXvDkAuQEPkO/WELzAHaoL+/V9iGwrUIm/DRzOEy04TLmisH9OJTbzX52TmnfFDpOEki55v2dEFj8nrN1SE3iwKivGOoEvth1FShNmdROVTTw+AQcHMdzOQm2eXlNlFY8+Co+LYb5bbJC5bdpHbx+bkUj34GoSQ7BrrToCdUxkwjCOW3/L/RlAfiDGl6ET3Psc6qrLAH2UqdKSpYcJFVNkoJUPIyYdT1iUzj7FwryTjQlOdUecTmMUgryQftTLDj3rRTb8lwgJpEL6xDQ5yyn4xJbVOUPH5Df70AHxI6Onw9Zv6OTrND9RKI7zLxRy8FmSdke6YQtCauyCJ0wNVIkP17vMqloRZ5rBiGsa3+Cf5LhAS9qvd/ghAgMBAAGgADANBgkqhkiG9w0BAQwFAAOCAYEANPqKVVKqegfsmbUBwfdh0cejBxnd8nG6SmEwQF2lO69FHrsFjN2OTjpFN8IywzpnWwjZmvzcP2FDeolnIunBrasWaw8YK8ULU+yrXYuY1GaSFyUcOhTAyfUB6mrm7IKvdv2mQ9wRSI8nUVmH/G7LQSBda6dDGilvNo7DuKqbQsSYFDsPDRtnVjW63GhfjIqscW086w7hXTpwUCqc8yTMOJ3KNdpHbg3gSBo0W66NfgCu9JIJNbODG4bCq6Lo3MwcRe1Ps6rmykhmKRYh5ZgmCZeySQwoyO/UM7UM/i/Zk3ekdyo2M211P728888+nLuuy0LsOsqiRDREg7ehWixE+1Oa1IZath0c+mIp+o7zTq/LEdF4adUwCtAXFuV9C0zo0xCWanQI8l8To0FTJbAA4OLOWptY/L6/uDMDvZPayTRaWk7kKb8d4k/W3qiRxlVNaf2Xt4wIWK9iB63vz8fav4CD92YK2pYGsoItU08giTvZlqLQi871W4jKOa2GaarhV)

FCS_CKM.2	Admin table (Generated TLS server credential)	Date: 09/01/20 09:04:54 CDT Client: 127.0.0.1 Category: system Client ID: Installer Event: Generated key pair and certificate request on HSM for TLS; Request: (Subject: CN=192.168.144.161, O=ISC, C=US; Base64-encoded: MIIDejCCAeICAQAwNTELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEYMBYGA1UEAxMPMTkyLjE2OC4xNDQuMTYxMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEArLGKQ/36L0P0akWUJh5+cSWKeuH/H/efqMT0V2jDVqyHBmUy/P3LyZwz3tOmtpzvShj4ALTFbNNmdLtd0mp0E7+3QCcjqxIIRdW3QB2u1IJXOIr076qMrU0iDcwreBSpL2qiUWH48wcXvDkAuQEPkO/WELzAHaoL+/V9iGwrUIm/DRzOEy04TLmisH9OJTbzX52TmnfFDpOEki55v2dEFj8nrN1SE3iwKivGOoEvth1FShNmdROVTTw+AQcHMdzOQm2eXlNlFY8+Co+LYb5bbJC5bdpHbx+bkUj34GoSQ7BrrToCdUxkwjCOW3/L/RlAfiDGl6ET3Psc6qrLAH2UqdKSpYcJFVNkoJUPIyYdT1iUzj7FwryTjQlOdUecTmMUgryQftTLDj3rRTb8lwgJpEL6xDQ5yyn4xJbVOUPH5Df70AHxI6Onw9Zv6OTrND9RKI7zLxRy8FmSdke6YQtCauyCJ0wNVIkP17vMqloRZ5rBiGsa3+Cf5LhAS9qvd/ghAgMBAAGgADANBgkqhkiG9w0BAQwFAAOCAYEANPqKVVKqegfsmbUBwfdh0cejBxnd8nG6SmEwQF2lO69FHrsFjN2OTjpFN8IywzpnWwjZmvzcP2FDeolnIunBrasWaw8YK8ULU+yrXYuY1GaSFyUcOhTAyfUB6mrm7IKvdv2mQ9wRSI8nUVmH/G7LQSBda6dDGilvNo7DuKqbQsSYFDsPDRtnVjW63GhfjIqscW086w7hXTpwUCqc8yTMOJ3KNdpHbg3gSBo0W66NfgCu9JlJNbODG4bCq6Lo3MwcRe1Ps6rmykhmKRYh5ZgmCZeySQwoyO/UM7UM/i/Zk3ekdyo2M211P72888+nLuuy0LsOsqiRDREg7ehWixE+1Oa1IZath0c+mIp+o7zTq/LEdF4adUwCtAXFuV9C0zo0xCWanQI8l8To0FTJbAA4OLOWptY/L6/uDMDvZPayTRaWk7kKb8d4k/W3qiRxlVNaf2Xt4wIWK9iB63vz8fav4CD92YK2pYGsoItU08giTvZlqLQi871W4jKOa2GaarhV) Admin table (Generated initial authentication credential)	Date: 09/01/20 09:04:55 CDT Client: 127.0.0.1 Category: system Client ID: Installer Event: Generated key pair and certificate request for administrator; Request: (Subject: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US; Base64-encoded: MIIDiDCCAfACAQAwQzELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEmMCQGA1UEAxMdQ2VydEFnZW50IDcuMC45IEFkbWluaXN0cmF0b3IwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDNT0XGYcpgD8HgTPN9S7XllwTze+dtAiUACtCUl1Zf5kdlJ/W5Kf91c0e4Ota9o5dgv5d85/UFxq/lxcwEF7uLQRY6c5mz1d/7yYFE8HfnkUtWkmLkmOxeBE8i7LAVTHQneljOA/yE/YjBYIne15lQD38nJ/Y18N45tbVXEHcaON/T5y9huKCEbp9G+1SVgvmP2NrYGY/r580xVafUZk+/5SFhYtnAiwlFHy1WDdTHb/A4j8aZpa3z3N+H5NT3YJyGcY0XuhypnomvIxJTBwgA5XNikj6etOsVf8nZqeb006O0ABbebjl1Ih+c0LpyWdAzY8Ybq1210eBc7Gf1Oag17GAKPBr1+UGCOZGMoYpgRceZjC/9ktSoJlcYE3RJfKJhDMhdCdc9Htd3CR985LDYs8ZdL+EVSPcjjzPHgi8DQ/sBfTHlj35RkiRxZ8qsNxMVA1i8UuAfCrMC1R8tfJ1pt/P7MBxaUp8QLVFOdcayt+BaJlUKHEwMDdauBSn2FucCAwEAAaAAMA0GCSqGSIb3DQEBDAUAA4IBgQAw0H8yQ9TAYT7ngXjirF1SgRYe9IPUyuQsU7xGER4YletCX6/L/TbmVqfdBoa5QCgpBsw+5QMRWBqmMnJpEMwXBmv4Ejr/pllYsldy+ow4tAkJNVe+aEfQwkeHXJs1YVcKTQO/CpdtwD4Ovsema62W2yjcnWBv3P2JsqN028GFAO87Nm3KwtZeM2m/rQcAtIRSJGmkngu8qRyADzorYoPSqhaj6yKSaPdDJREMR/tnT79aUfmUbaRpf+9dRgprDJUQhD+xLlcN9CGdov1u3z7JubCMErPRDDbdKGtfCsWAJWuhQDTyBeGCue5TgiSQMmfO47x8Ey8BQh4jzn/Cj09VKiNeP9B97L3OiJAOlWNpymCFoOpWgTqDvSj0zSKI+rcckvbZt84YjxFprkfBnF+M9w767R/86+8+fhoD68uIzy0OXfBBsOpvHSS+NIgIUbdua+SaSjIfOLuGkdaOWf81MiNHjjP0tE8RMVev1/rlOooKAbIyEJOLJPLOoPOomKQ=)

	Admin table (Generated an issuer credential)	Date: 09/01/20 09:04:52 CDT Client: 127.0.0.1 Category: system Client ID: Installer Event: Generated a new root credential and applied it to CA: ca7; Certificate: (Serial: 3CE4F100000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Base64-encoded: MIIEdTCCAt2gAwIBAgIUPOTxAAAAAAAAAAAAAAAAAAAAEwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDA5MDExNDA0NDVaFw0yNTA5MDExNDA0NDVaMEIxCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxJTAjBgNVBAMTHENlcnRBZ2VudCA3LjAuOSBSb290IENBIERDQjcwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQCXMTjkOcd+lIAuGh7lwgg3qr3KGSaEtveU/8vZBfFUU+HGfM1yIn6kqvCtxvdjuvDOU1zsXXAkAwno6Clx1sR9SHkYjwwL9zPscYl/5+jitypYugVS67vwUKsmqULexWdpIerVcKi7oqeKHjfcH8BIxCKflweP0poF2nIq+T6/k4wfjjTjmizwGJvm/C7dq2DTPLy3pW48pkbquvXUWMTYLj+UsejSYunMDn/ilkRbcvN+QSzjTTRmDmV6mRFde9Z8C1E7cPY/QjIMtN1P9Jx77CLIWZc3FKNSXLCQgPqqB7AiLJPF8EsoaLCaT/wVNMWqOs0sgnloyv/mWwmT5XO/jE6K9/4Wf6nJpH4+RJrunVIwjL6YQyF/FehosdFPhsyOPyxm6Kk8qv4G2b6w2VLxbY5Fhcpc+2EiezBGQ8P3u4cyNltc52BQ/8x3vPS3f9l5tQ9VDDsNN4QQIeAaEPOblSq2D3Sx7SJrRKSckBZ1Oy/u/T7jBGBDhuQmtVO+M6kCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFMv64F1e8ZnGJGHlXZ4tHOD/ZVq7MB8GA1UdIwQYMBaAFMv64F1e8ZnGJGHlXZ4tHOD/ZVq7MA0GCSqGSIb3DQEBDAUAA4IBgQAoE+IBm+QqHJOkkcGvNmhb06tBgsi7gStTJbQpTLO4a/MGZP4DLpFn1zIQnpCStWVXfeGY2+aQNee/eRZ15uzv6Un+ws0tsq6rv3rHIGuYmXS26WdH9MAPTjL9MQkfkGz+4WSeudRZn4luiWLCdGU9QqK5MQUTreY8MQAUz0NbvlfOBL8XX4aB+oGlECACpLj1ZOWvc6au30JKiQwrtmGadR2NnvR5W9knD6YuxTmy9NJpPrAnIqiBd0j772IWCzqlSBWqkTyZbFicb7aqw9UVx5XcK2Yvxj5PnAdMmkSCm5XpglsLscXQPqGIZ3H4CxhZffaxWTKLqTa2oGvLr4l6niN5IfqbIdh9nUw1NxVmnCByP4uBRGD+vOAWk1WGUSMK6lW0wPYc0IwvR8Z0Ogg6/MaXWiee1Z/LTQKXGyiuzOxsUiKLZfxyls7YLnpDZUSXJvZeT9sHOiql0vVA8swkQCzVr9OBaKDqwGxc2K3GUdilPnIuheDfsnkauQ/oTRY=); Request: (Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Base64-encoded: MIIDhzCCAe8CAQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAJcxOOQ5x36UgC4aHuXCCDeqvcoZJoS295T/y9kF8VRT4cZ8zXIifqSq8K3G92O68M5TXOxdcCQDCejoKXHWxH1IeRiPDAv3M+xxiX/n6OK3Kli6BVLru/BQqyapQt7FZ2kh6tVwqLuip4oeN9wfwEjEIp+XB4/SmgXacir5Pr+TjB+ONOOaLPAYm+b8Lt2rYNM8vLelbjymRuq69dRYxNguP5Sx6NJi6cwOf+KWRFty835BLONNNGYOZXqZEV171nwLUTtw9j9CMgy03U/0nHvsIshZlzcUo1JcsJCA+qoHsCIsk8XwSyhosJpP/BU0xao6zSyCeWjK/+ZbCZPlc7+MTor3/hZ/qcmkfj5Emu6dUjCMvphDIX8V6Gix0U+Gzl4/LGboqTyq/gbZvrDZUvFtjkWFylz7YSJ7MEZDw/e7hzI2W1znYFD/zHe89Ld/2Xm1D1UMOw03hBAh4BoQ85uVKrYPdLHtImtEpJyQFnU7L+79PuMEYEOG5Ca1U74zqQIDAQABoAAwDQYJKoZIhvcNAQEMBQADggGBAESsmxSgbAVngGjWB2UAGBBIsMkgTAGrzTca9Nqv3F4VQqkDeYkIKs6vgcsH45QBoFUCdNwtGuVyZc0GZahy5rNBDYVGxcTe9rOInoHS1gJqQjb9cXR36yHaBI2KM5dwaDVAtqEGhA0Hj9uRkdVXKL06zMkJ0V6XCFCbBAq8RIYBWfVdalghC3yWIZtfRyhJSVrVjlxbxvmpx48TOss0eZ2XceAuqoE9TdhB8hgd6XRNcfdfSJoFIyaHC5UU1Rtg95KX+tAk7ceqvB5NIuU1qT/5bPg94w+LRAyILXBFMHEVn5YcrWJYNNNFpB7PdzWQu/R4E5B66ZUJmiAQkHIFEw2Sa7YjH9dEZyKmnEN9wpF/NJJ2HjFg1oQRd3kR1dbGV8ae1ipzEZl5/BltbTCdV7l1jOD0tAX1mCpPvXCuOJENTIoPfTgaBNkFrur2WKEkoSLQBgpxQAKKKFmyGY8WWKUNuTnpjDX9+d9b5nD2l1YBI74rC2oAzQYDeq7ERYpOpg==)

FCS_CKM_EXT.5	Admin table (Integrity failure on trust anchor DB)	Date: 09/01/20 12:18:12 CDT Client: [system] Category: System Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Fatal error; Fatal error occurred at ccPathValidationIfEnabled. CertAgent will be shut down. Error: Path validation failed. Cannot verify the integrity of the Trust Anchor database; Signature failure
	Admin table (Integrity failure on ACL DB)	Date: 09/01/20 12:28:12 CDT Client: [system] Category: System Client ID: (n/a) Event: Fatal error; Fatal error occurred at caGetAuthCAComboTag. CertAgent will be shut down. Error: Cannot verify the integrity of the ACL database; Signature failure

FCS_COP.1(2)	Admin table (Generated an issuer credential)	Date: 09/01/20 09:04:52 CDT Client: 127.0.0.1 Category: system Client ID: Installer Event: Generated a new root credential and applied it to CA: ca7; Certificate: (Serial: 3CE4F100000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Base64-encoded: MIIEdTCCAt2gAwIBAgIUPOTxAAAAAAAAAAAAAAAAAAAAEwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDA5MDExNDA0NDVaFw0yNTA5MDExNDA0NDVaMEIxCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxJTAjBgNVBAMTHENlcnRBZ2VudCA3LjAuOSBSb290IENBIERDQjcwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQCXMTjkOcd+lIAuGh7lwgg3qr3KGSaEtveU/8vZBfFUU+HGfM1yIn6kqvCtxvdjuvDOU1zsXXAkAwno6Clx1sR9SHkYjwwL9zPscYl/5+jitypYugVS67vwUKsmqULexWdpIerVcKi7oqeKHjfcH8BIxCKflweP0poF2nIq+T6/k4wfjjTjmizwGJvm/C7dq2DTPLy3pW48pkbquvXUWMTYLj+UsejSYunMDn/ilkRbcvN+QSzjTTRmDmV6mRFde9Z8C1E7cPY/QjIMtN1P9Jx77CLIWZc3FKNSXLCQgPqqB7AiLJPF8EsoaLCaT/wVNMWqOs0sgnloyv/mWwmT5XO/jE6K9/4Wf6nJpH4+RJrunVIwjL6YQyF/FehosdFPhsyOPyxm6Kk8qv4G2b6w2VLxbY5Fhcpc+2EiezBGQ8P3u4cyNltc52BQ/8x3vPS3f9l5tQ9VDDsNN4QQIeAaEPOblSq2D3Sx7SJrRKSckBZ1Oy/u/T7jBGBDhuQmtVO+M6kCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFMv64F1e8ZnGJGHlXZ4tHOD/ZVq7MB8GA1UdIwQYMBaAFMv64F1e8ZnGJGHlXZ4tHOD/ZVq7MA0GCSqGSIb3DQEBDAUAA4IBgQAoE+IBm+QqHJOkkcGvNmhb06tBgsi7qStTJbQpTLO4a/MGZP4DLpFn1zIQnpCStWVXfeGY2+aQNee/eRZ15uzv6Un+ws0tsq6rv3rHIGuYmXS26WdH9MAPTjL9MQkfkGz+4WSeudRZn4luiWLCdGU9QqK5MQUTreY8MQAUz0NbvlfOBL8XX4aB+oGlECACpLj1ZOWvc6au30JKiQwrtmGadR2NnvR5W9knD6YuxTmy9NJpPrAnIqiBd0j772IWCzqlSBWqkTyZbFicb7aqw9UVx5XcK2Yvxj5PnAdMmkSCm5XpglsLscXQPqGlZ3H4CxhZffaxWTKLqTa2oGvLr4l6niN5IfqbIdh9nUw1NxVmnCByP4uBRGD+vOAWk1WGUSMK6lW0wPYc0IwvR8Z0Ogg6/MaXWiee1Z/LTQKXGyiuzOxsUiKLZfxyls7YLnpDZUSXJvZeT9sHOiql0vVA8swkQCzVr9OBaKDqwGxc2K3GUdilPnIuheDfsnkauQ/oTRY=); Request: (Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Base64-encoded: MIIDhzCCAe8CAQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAJcxOOQ5x36UgC4aHuXCCDeqvcoZJoS295T/y9kF8VRT4cZ8zXIifqSq8K3G92O68M5TXOxdcCQDCejoKXHWxH1IeRiPDAv3M+xxiX/n6OK3Kli6BVLru/BQqyapQt7FZ2kh6tVwqLuip4oeN9wfwEjEIp+XB4/SmgXacir5Pr+TjB+ONOOaLPAYm+b8Lt2rYNM8vLelbjymRuq69dRYxNguP5Sx6NJi6cwOf+KWRFty835BLONNNGYOZXqZEV171nwLUTtw9j9CMgy03U/0nHvsIshZlzcUo1JcsJCA+qoHsCIsk8XwSyhosJpP/BU0xao6zSyCeWjK/+ZbCZPlc7+MTor3/hZ/qcmkfj5Emu6dUjCMvphDIX8V6Gix0U+Gzl4/LGboqTyq/gbZvrDZUvFtjkWFylz7YSJ7MEZDw/e7hzI2W1znYFD/zHe89Ld/2Xm1D1UMOw03hBAh4BoQ85uVKrYPdLHtImtEpJyQFnU7L+79PuMEYEOG5Ca1U74zqQIDAQABoAAwDQYJKoZIhvcNAQEMBQADggGBAESsmxSgbAVngGjWB2UAGBBIsMkgTAGrzTca9Nqv3F4VQqkDeYkIKs6vgcsH45QBoFUCdNwtGuVyZc0GZahy5rNBDYVGxcTe9rOInoHS1gJqQjb9cXR36yHaBI2KM5dwaDVAtqEGhA0Hj9uRkdVXKL06zMkJ0V6XCFCbBAq8RIYBWfVdalghC3yWIZtfRyhJSVrVjlxbxvmpx48TOss0eZ2XceAuqoE9TdhB8hgd6XRNcfdfSJoFIyaHC5UU1Rtg95KX+tAk7ceqvB5NIuU1qT/5bPg94w+LRAyILXBFMHEVn5YcrWJYNNNFpB7PdzWQu/R4E5B66ZUJmiAQkHIFEw2Sa7YjH9dEZyKmnEN9wpF/NJJ2HjFg1oQRd3kR1dbGV8ae1ipzEZl5/BltbTCdV7l1jOD0tAX1mCpPvXCuOJENTIoPfTgaBNkFrur2WKEkoSLQBgpxQAKKKFmyGY8WWKUNuTnpjDX9+d9b5nD2l1YBI74rC2oAzQYDeq7ERYpOpg==)

	CA table (Issued a certificate)	Date: 09/01/20 13:07:04 CDT Client: 10.1.10.194 Category: request Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 211426C5C8A861466C9E782099B9564E84EE785F; Certificate: (Serial: 7692F800000000000000000000000000000001C; Subject: CN=NIAP Test User 2, O=ISC, C=US); Signer: (Serial: 3CE4F1000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)
	CA table (Issued a CRL)	Date: 09/01/20 13:17:04 CDT Client: 10.1.10.194 Category: CRL Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Issued CRL; Signer: (Serial: 3CE4F1000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)
	CA table (Signed OCSP response)	Date: 09/01/20 13:13:05 CDT Client: 10.1.10.194 Category: OCSP Client ID: (n/a) Event: Processed OCSP request; Serial: 52FEF10000000000000000000000000000016; returned status: GOOD; Signer: (Serial: 35383E00000000000000000000000000000006; Subject: CN=CertAgent 7.0.9 OCSP Signer, O=ISC, C=US)
	CA table (Issued a certificate via RAMI)	Date: 09/01/20 13:15:15 CDT Client: 127.0.0.1 Category: RAMI Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 3FB2093A9794F900B49A9AC836E307A4C96CF370; Certificate: (Serial: 3B76B80000000000000000000000000000000008; Subject: CN=CertAgent Key Enrollment Test, O=ISC, C=US); Signer: (Serial: 3CE4F1000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)

	CA table (Signed EST response)	Date: 09/01/20 13:40:55 CDT Client: 10.1.10.194 Category: EST Client ID: EST User Event: Processed EST simpleenroll request: Request ID: 412B736D737223BE6B34CB49B07D772ECF560B0C; Certificate: (Serial: 5B6F58000000000000000000000000000000000008; Subject: CN=EST User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); Client: EST User; EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzIs+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGgDzANBgkqhkiG9w0BCQ4xADANBgkqhkiG9w0BAQwFAAOCAYEAI9XAor3MpQh2VC48nauw7EDJEjfUbhQZx90YQT7pYTLddOOT9BGY8LED0JcTM/2sfdjX9hEwIdX9qHWRUs0h/5OtQvnz6BixYViMFgA1BqLIH9qtiNvdvQNz9D476+qbFGmSqxcfirBsxqDgygZK1VDY/ajKUv/ZZiGmWO6Zdj7pDobkPNIhYTFiuhORl08tNJjRM1fuO7AiCUDuID0joXcVjdgztxAI0CAZJfsFA82EnVUsM5I76OnXslbpNT03QQan8e7m4U5oR/53LPN/jJ4tr9wpuJs7CLiH1qWeffTsMyJwcelSasb7/hMyWTM0lGOcAUxbLtUD2cQVC+WzO0AY5Jh7RviBcPluSK+S1dNBHYD2DwmDpwhFYU/u5Mit/s1rr/ILXtsX+hsSsm/8zDEM+hFgWK5OP5Qm3ufGwvUvCr/Hf9PTf/NpVVt14FY1remQptrDYm6jTM+R/xC8KVRBNe652kJ29m8+D2EZhZV/zNnbaqduTe6waOwOUWjO; EST Response (200): MIIEbwYJKoZIhvcNAQcCoIIEYDCCBFwCAQExADALBgkqhkiG9w0BBwGgggREMIIEQDCCAqigAwIBAgIUW29YAAAAAAAAAAAAAAAAAAAAAAAwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDA5MDExODQwNTVaFw0yNTA5MDExNDA0NDVaMC4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzIs+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGjQjBAMB0GA1UdDgQWBBTTI9rktiax6I8u00yRFulurpck4jAfBgNVHSMEGDAWgBTL+uBdXvGZxiRh5V2eLRzg/2VauzANBgkqhkiG9w0BAQwFAAOCAYEAYrAgpVasq0ELgeLdcWUFTD8+9ab3HXID54BoT7A+WLEUuHO6q9hKBG/x98MmjqijuVymdx507ktHGYXEFKV4FCv2fS9QKBaRPhJccSp1nYRWr4zERiH7s4zRy5xhtJG6Ebq+xaRWJHUWf3gmC4G7iaMz1dnMD/Yt0p7Vozy7tftsMH727chporjQpxpd37RvVdMoouRq9I5RolEQy0pxhq6oSzR7ksFWEviuVwfJAFB3tVGH/6MddUwMjBGUmA2eWF+sOVVhX529tGFpQLcrZoHknKiBc5xkBWpb3dKg5B3kGlgXMkqliuGUoWNSeyTac0WhaVcIfJjokG+tr7/XgmJZcHky7gkI6vxCbcYjoNmKRPBG83wRknWqwIziKZuodkJi/pko/GoVs3UUKn9Aq9bt+8PeCPCBG/vC8V6TZx9gjmVt8afDp0uK7RO087jmVQPYJ8CMstbV7RqnCf17dmBbYoYSPfa881cvJcJdIbp7f2JzdpO560OydkwmdRFVMQA= Client: 10.1.10.194 Category: EST Client ID: EST User Event: Processed EST simpleenroll request: Request ID: 412B736D737223BE6B34CB49B07D772ECF560B0C; Certificate: (Serial: 5B6F58000000000000000000000000000000000008; Subject: CN=EST User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); Client: EST User; EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzIs+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGjQjBAMB0GA1UdDgQWBBTTI9rktiax6I8u00yRFulurpck4jAfBgNVHSMEGDAWgBTL+uBdXvGZxiRh5V2eLRzg/2VauzANBgkqhkiG9w0BAQwFAAOCAYEAYrAgpVasq0ELgeLdcWUFTD8+9ab3HXID54BoT7A+WLEUuHO6q9hKBG/x98MmjqijuVymdx507ktHGYXEFKV4FCv2fS9QKBaRPhJccSp1nYRWr4zERiH7s4zRy5xhtJG6Ebq+xaRWJHUWf3gmC4G7iaMz1dnMD/Yt0p7Vozy7tftsMH727chporjQpxpd37RvVdMoouRq9I5RolEQy0pxhq6oSzR7ksFWEviuVwfJAFB3tVGH/6MddUwMjBGUmA2eWF+sOVVhX529tGFpQLcrZoHknKiBc5xkBWpb3dKg5B3kGlgXMkqliuGUoWNSeyTac0WhaVcIfJjokG+tr7/XgmJZcHky7gkI6vxCbcYjoNmKRPBG83wRknWqwIziKZuodkJi/pko/GoVs3UUKn9Aq9bt+8PeCPCBG/vC8V6TZx9gjmVt8afDp0uK7RO087jmVQPYJ8CMstbV7RqnCf17dmBbYoYSPfa881cvJcJdIbp7f2JzdpO560OydkwmdRFVMQA=
	CA table (Failed to issue a CRL)	Date: 09/01/20 13:47:58 CDT Client: 10.1.10.194 Category: CRL Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Cannot issue CRL; error: Cannot initialize the PKCS11 library; error: Card not found; HSM library: /usr/safenet/lunaclient/lib/libCryptoki2_64.so

FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1, and FCS_TLSS_EXT.2	Admin table	Date: 09/01/20 09:32:13 CDT Client: 10.1.10.194 Category: TLS session Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Established trusted channel
		Date: 09/01/20 09:35:17 CDT Client: 10.1.10.194 Category: TLS session Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Terminated trusted channel
		Date: 09/01/20 09:36:27 CDT Client: 10.1.10.194 Category: TLS session Client ID: (n/a) Event: Cannot establish trusted channel; error: Client requested protocol TLSv1.1 is not enabled or supported in server context
		Date: 09/01/20 09:38:11 CDT Client: 10.1.10.194 Category: TLS session Client ID: (n/a) Event: Cannot establish trusted channel; error: Client DN does not match DN filter: CN=Test User, O=ISC, C=US
FDP_CER_EXT.1	CA table (Issued a certificate via web interface)	Date: 09/01/20 10:18:17 CDT Client: 10.1.10.194 Category: request Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 211426C5C8A861466C9E782099B9564E84EE785F; Certificate: (Serial: 7692F8000000000000000000000000000000001C; Subject: CN=NIAP Test User 2, O=ISC, C=US); Signer: (Serial: 3CE4F1000000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)
	CA table (Issued a certificate via RAMI)	Date: 09/01/20 10:39:31 CDT Client: 127.0.0.1 Category: RAMI Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 3FB2093A9794F900B49A9AC836E307A4C96CF370; Certificate: (Serial: 3B76B8000000000000000000000000000000000008; Subject: CN=CertAgent Key Enrollment Test, O=ISC, C=US); Signer: (Serial: 3CE4F1000000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)

	CA table (Issued a certificate via EST)	Date: 09/01/20 13:40:55 CDT Client: 10.1.10.194 Category: EST Client ID: EST User Event: Processed EST simpleenroll request: Request ID: 412B736D737223BE6B34CB49B07D772ECF560B0C; Certificate: (Serial: 5B6F58000000000000000000000000000000000008; Subject: CN=EST User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); Client: EST User; EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzIs+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGgDzANBgkqhkiG9w0BCQ4xADANBgkqhkiG9w0BAQwFAAOCAYEAI9XAor3MpQh2VC48nauw7EDJEjfUbhQZx90YQT7pYTLddOOT9BGY8LED0JcTM/2sfdjX9hEwIdX9qHWRUs0h/5OtQvnz6BixYViMFgA1BqLIH9qtiNvdvQNz9D476+qbFGmSqxcfirBsxqDgygZK1VDY/ajKUv/ZZiGmWO6Zdj7pDobkPNIhYTFiuhORl08tNJjRM1fuO7AiCUDuID0joXcVjdgztxAI0CAZJfsFA82EnVUsM5I76OnXslbpNT03QQan8e7m4U5oR/53LPN/jJ4tr9wpuJs7CLiH1qWeffTsMyJwcelSasb7/hMyWTM0lGOcAUxbLtUD2cQVC+WzO0AY5Jh7RviBcPluSK+S1dNBHYD2DwmDpwhFYU/u5Mit/s1rr/ILXtsX+hsSsm/8zDEM+hFgWK5OP5Qm3ufGwvUvCr/Hf9PTf/NpVVt14FY1remQptrDYm6jTM+R/xC8KVRBNe652kJ29m8+D2EZhZV/zNnbaqduTe6waOwOUWjO; EST Response (200): MIIEbwYJKoZIhvcNAQcCoIIEYDCCBFwCAQExADALBgkqhkiG9w0BBwGgggREMIIEQDCCAqigAwIBAgIUW29YAAAAAAAAAAAAAAAAAAAAAAAwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDA5MDExODQwNTVaFw0yNTA5MDExNDA0NDVaMC4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzIs+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGjQjBAMB0GA1UdDgQWBBTTI9rktiax6I8u00yRFulurpck4jAfBgNVHSMEGDAWgBTL+uBdXvGZxiRh5V2eLRzg/2VauzANBgkqhkiG9w0BAQwFAAOCAYEAYrAgpVasq0ELgeLdcWUFTD8+9ab3HXID54BoT7A+WLEUuHO6q9hKBG/x98MmjqijuVymdx507ktHGYXEFKV4FCv2fS9QKBaRPhJccSp1nYRWr4zERiH7s4zRy5xhtJG6Ebq+xaRWJHUWf3gmC4G7iaMz1dnMD/Yt0p7Vozy7tftsMH727chporjQpxpd37RvVdMoouRq9I5RolEQy0pxhq6oSzR7ksFWEviuVwfJAFB3tVGH/6MddUwMjBGUmA2eWF+sOVVhX529tGFpQLcrZoHknKiBc5xkBWpb3dKg5B3kGlgXMkqliuGUoWNSeyTac0WhaVcIfJjokG+tr7/XgmJZcHky7gkI6vxCbcYjoNmKRPBG83wRknWqwIziKZuodkJi/pko/GoVs3UUKn9Aq9bt+8PeCPCBG/vC8V6TZx9gjmVt8afDp0uK7RO087jmVQPYJ8CMstbV7RqnCf17dmBbYoYSPfa881cvJcJdIbp7f2JzdpO560OydkwmdRFVMQA=

FDP_CER_EXT.2	CA table	Date: 09/01/20 10:18:17 CDT Client: 10.1.10.194 Category: request Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 211426C5C8A861466C9E782099B9564E84EE785F; Certificate: (Serial: 7692F8000000000000000000000000000000001C; Subject: CN=NIAP Test User 2, O=ISC, C=US); Signer: (Serial: 3CE4F1000000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)
		Date: 09/01/20 13:58:27 CDT Client: 10.1.10.194 Category: request Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Cannot link certificate (Serial: 5B6F5800000000000000000000000000000008) to request (ID: 412B736D737223BE6B34CB49B07D772ECF560B0E; error: Cannot find request matches the request ID
FDP_CER_EXT.3	CA table (Failed to approve via UI)	Date: 09/01/20 13:00:57 CDT Client: 10.1.10.194 Category: request Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Cannot process request: Request ID: 36B5735707BF73C4FD71198DFE5052F083AD132D; Signer: (Serial: 3CE4F1000000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); error: RSA 4096 certificate request is not acceptable. Acceptable key types and sizes: RSA 3072 only , NIST P-256, and NIST P-384
	CA table (Failed to approve via RAMI)	Date: 09/01/20 13:05:02 CDT Client: 10.1.10.194 Category: RAMI Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Cannot process RAMI request; error: Invalid PKCS#10 certificate request; Invalid signature

	CA table (Failed to approval via EST)	Date: 09/01/20 13:37:41 CDT Client: 10.1.10.194 Category: EST Client ID: EST User2 Event: Cannot process EST simpleenroll request; error: Unauthorized; Invalid user name (EST User2) and/or password; Client: EST User2; EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjlqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzls+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGgDzANBgkqhkiG9w0BCQ4xADANBgkqhkiG9w0BAQwFAAOCAYEAI9XAor3MpQh2VC48nauw7EDJEjfUbhQZx90YQT7pYTLddOOT9BGY8LED0JcTM/2sfdjX9hEwIdX9qHWRUs0h/5OtQvnz6BixYViMFgA1BqLIH9qtiNvdvQNz9D476+qbFGmSqxcfirBsxqDgygZK1VDY/ajKUv/ZZiGmWO6Zdj7pDobkPNIhYTFiuhORl08tNJjRM1fuO7AiCUDuID0joXcVjdgztxAI0CAZJfsFA82EnVUsM5I76OnXslbpNT03QQan8e7m4U5oR/53LPN/jJ4tr9wpuJs7CLiH1qWeffTsMyJwcelSasb7/hMyWTM0lGOcAUxbLtUD2cQVC+WzO0AY5Jh7RviBcPluSK+S1dNBHYD2DwmDpwhFYU/u5Mit/s1rr/ILXtsX+hsSsm/8zDEM+hFgWK5OP5Qm3ufGwvUvCr/Hf9PTf/NpVVt14FY1remQptrDYm6jTM+R/xC8KVRBNe652kJ29m8+D2EZhZV/zNnbaqduTe6waOwOUWjO; EST Response (400): Cannot process EST simpleenroll request; error: Unauthorized; Invalid user name (EST User2) and/or password
FDP_STG_EXT.1	Admin table	Date: 09/01/20 09:39:55 CDT Client: 10.1.10.194 Category: NIAP Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Added trust anchor: Certificate: (Serial: 0x27DCACD6A75BC2705D6C2EF5F84AF0CCE619ABCA; Subject: CN=ISC Demo Root CA, O=ISC, C=US; Base64-encoded: MIICGjCCAYOgAwIBAgIUJ9ys1qdbwnBdbC71+ErwzOYZq8owDQYJKoZIhvcNAQEFBQAwNjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEZMBcGA1UEAxMQSVNDIERlbW8gUm9vdCBDQTAgFw0xMTA5MDgxNjM0MDZaGA8yMTExMDkwNzE2MzQwNlowNjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEZMBcGA1UEAxMQSVNDIERlbW8gUm9vdCBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA13U3sWgyrS5PCWOuP9xOVqSFDRSt1VafNmAztJvyri5pAk0a5C65UxLYR/5bqA7naVHyC+ooJ2mf6qDazbpF44eUJaxe1QNdVkhekvjrZTbxgUhGrMu1+91m+IUCO5d8LlQxtKsCNNk3ej+fiFPXCru0N6crO+HXJv4psC37mzkCAwEAAaMjMCEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQEFBQADgYEAaux5RHUifGK5y0nqDei1vUHNPNMDvWSH5VDW+TQxlOeo5/VQuwzIolTrcFvtwau7ctXX4bcrnNts087Eafx8mDE0qDmct/HnY51/0OB6TxMA8qKI5WAsqjun07hHiodBa/obSZYPLrFumeoVDD5Pf+bwvOFGoY7686GHjJMjtL4=)

		Date: 09/01/20 09:41:52 CDT Client: 10.1.10.194 Category: NIAP Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Removed trust anchor: Certificate: (Serial: 27DCACD6A75BC2705D6C2EF5F84AF0CCE619ABCA; Subject: CN=ISC Demo Root CA, O=ISC, C=US; Base64-encoded: MIICGjCCAYOgAwIBAgIUJ9ys1qdbwnBdbC71+ErwzOYZq8owDQYJKoZIhvcNAQEFBQAwNjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEZMBcGA1UEAxMQSVNDIERlbW8gUm9vdCBDQTAgFw0xMTA5MDgxNjM0MDZaGA8yMTExMDkwNzE2MzQwNlowNjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzEZMBcGA1UEAxMQSVNDIERlbW8gUm9vdCBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA13U3sWgyrS5PCWOuP9xOVqSFDRSt1VafNmAztJvyri5pAk0a5C65UxLYR/5bqA7naVHyC+ooJ2mf6qDazbpF44eUJaxe1QNdVkhekvjrZTbxgUhGrMu1+91m+IUCO5d8LlQxtKsCNNk3ej+fiFPXCru0N6crO+HXJv4psC37mzkCAwEAAaMjMCEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQEFBQADgYEAaux5RHUifGK5y0nqDei1vUHNPNMDvWSH5VDW+TQxlOeo5/VQuwzIolTrcFvtwau7ctXX4bcrnNts087Eafx8mDE0qDmct/HnY51/0OB6TxMA8qKI5WAsqjun07hHiodBa/obSZYPLrFumeoVDD5Pf+bwvOFGoY7686GHjJMjtL4=)
FDP_CRL_EXT.1	CA table	Date: 09/01/20 09:45:42 CDT Client: 10.1.10.194 Category: CRL Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Cannot issue CRL; error: Cannot initialize the PKCS11 library; error: Card not found; HSM library: /usr/safenet/lunaclient/lib/libCryptoki2_64.so
FDP_OCSPG_EXT.1	CA table	Date: 09/01/20 09:46:32 CDT Client: 10.1.10.194 Category: OCSP Client ID: (n/a) Event: Cannot process OCSP request; Serial: 7965F400000000000000000000000000000015; error: Cannot initialize the PKCS11 library; error: Card not found; HSM library: /usr/safenet/lunaclient/lib/libCryptoki2_64.so
FIA_X509_EXT.1 and FIA_X509_EXT.2	Admin table	Date: 09/01/20 09:55:01 CDT Client: 10.1.10.194 Category: CA account Client ID: CN=CCTest, O=ISC, C=US Event: Cannot login to the CA Account site; error: Unauthorized; Path validation failed. Client Authentication purpose not asserted in the extendedKeyUsage extension: CN=CCTest, O=ISC, C=US
		Date: 09/01/20 09:55:01 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Login failed; error: Unauthorized; Path validation failed. Root certificate not trusted: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US

		Date: 09/01/20 17:20:52 CDT Client: [system] Category: system Client ID: Update Tool Event: Cannot verify update package: C:\admin\testupdate-noCodeSigningEKU.p7m; Signer: (Serial: 1965F60000000000000000000000000000000025; Subject: CN=Signer without code signing, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Validity: 09/01/20 15:34:07 CDT - 09/01/21 15:34:07 CDT); error: Cannot verify signer certificate with path validation; error: Path validation failed. Code Signing purpose not asserted in the extendKeyUsage extension: CN=Signer without code signing, O=ISC, C=US
FIA_UAU_EXT.1	CA table (Logged in to CA account)	Date: 09/01/20 10:25:13 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Logged in
	Admin table (Logged in to Admin site)	Date: 09/01/20 10:25:19 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Logged in
FIA_UIA_EXT.1	CA table (Logged in to CA account)	Date: 09/01/20 10:02:59 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Logged in
	Admin table (Failed to login to CA account)	Date: 09/01/20 10:05:49 CDT Client: 10.1.10.194 Category: CA account Client ID:CN=Test User 1, O=ISC, C=US Event: Cannot login to the CA Account site; error: Unauthorized
	Admin table (Logged in to Admin site)	Date: 09/01/20 10:03:42 CDT Client: 10.1.10.194 Category: login Client ID:CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Logged in
	Admin table (Failed to login to Admin site)	Date: 09/01/20 10:05:53 CDT Client: 10.1.10.194 Category: login Client ID: CN= Test User 1, O=ISC, C=US Event: Login failed; error: Unauthorized
	CA table (Issued cert via RAMI)	Date: 09/01/20 10:15:22 CDT Client: 10.1.10.194 Category: RAMI Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Processed request: Request ID: 4DB131C59AD7BA3DB75B3748E189BD54793404EF; Certificate: (Serial: 11034F000000000000000000000000000000000D; Subject: CN=RAMI User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US)

	CA table (Failed to access RAMI)	Date: 09/01/20 10:17:52 CDT Client: 10.1.10.194 Category: RAMI Client ID: CN=Test User 1, O=ISC, C=US Event: Cannot process RAMI request; error: You are not an authorized user
	CA table (Queried audit records via DBAccess)	Date: 09/01/20 10:19:24 CDT Client: 10.1.10.194 Category: DBACCESS Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Executed audit trail query: SELECT LDATE,TYPE,CLIENTID,EVENT FROM CA_AUDIT_CA7 order by LDATE DESC LIMIT 5
	CA table (Failed to query audit records via DBAccess)	Date: 09/01/20 10:23:31 CDT Client: 127.0.0.1 Category: DBACCESS Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Query failed: SELECT LDATE,TYPE,CLIENTID,EVENT FROM CA_AUDIT_CA7 order by LDATE DESC LIMIT 5; error: You are not an authorized user; 'dbaccess' permission is required

FIA_ESTS_EXT.1	CA table (Client Certificate Authentication)	Date: 09/01/20 13:46:59 CDT Client: 10.1.10.194 Category: EST Client ID: CN=EST User, O=ISC, C=US Event: Processed EST simpleenroll request: Request ID: 55273BCEA82E667A52F94D308CDE325472C0DEE9; Certificate: (Serial: 7EC1D50000000000000000000000000000000009; Subject: CN=EST User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); Client: (Serial: 5B6F58000000000000000000000000000000008; Subject: CN=EST User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzls+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGgDzANBgkqhkiG9w0BCQ4xADANBgkqhkiG9w0BAQwFAAOCAYEAI9XAor3MpQh2VC48nauw7EDJEjfUbhQZx90YQT7pYTLddOOT9BGY8LED0JcTM/2sfdjX9hEwIdX9qHWRUs0h/5OtQvnz6BixYViMFgA1BqLIH9qtiNvdvQNz9D476+qbFGmSqxcfirBsxqDgygZK1VDY/ajKUv/ZZiGmWO6Zdj7pDobkPNIhYTFiuhORl08tNJjRM1fuO7AiCUDuID0joXcVjdgztxAI0CAZJfsFA82EnVUsM5I76OnXslbpNT03QQan8e7m4U5oR/53LPN/jJ4tr9wpuJs7CLiH1qWeffTsMyJwcelSasb7/hMyWTM0lGOcAUxbLtUD2cQVC+WzO0AY5Jh7RviBcPluSK+S1dNBHYD2DwmDpwhFYU/u5Mit/s1rr/ILXtsX+hsSsm/8zDEM+hFgWK5OP5Qm3ufGwvUvCr/Hf9PTf/NpVVt14FY1remQptrDYm6jTM+R/xC8KVRBNe652kJ29m8+D2EZhZV/zNnbaqduTe6waOwOUWjO; EST Response (200): MIIEbwYJKoZIhvcNAQcCoIIEYDCCBFwCAQExADALBgkqhkiG9w0BBwGgggREMIIEQDCCAqigAwIBAgIUfsHVAAAAAAAAAAAAAAAAAAAAAAAwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDExMDQxNDMxMzNaFw0yNTA5MDExNDA0NDVaMC4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzls+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGjQjBAMB0GA1UdDgQWBBTTI9rktiax6I8u00yRFulurpck4jAfBgNVHSMEGDAWgBTL+uBdXvGZxiRh5V2eLRzg/2VauzANBgkqhkiG9w0BAQwFAAOCAYEAWT6vCRpbjcL6s1DLOnN+Mu9rikebp1oHzXJUgTsKEjbDxovLvYAKkuA14k+qLYdrl7EDBEbW07fZNejQ3lAssxYhYsEUg3AmvUtpxCajYHw41eHNuahrhPNCTBv97ZjnDqkqYMrZJ1LezKDoQQCl2QUjukoqTQcPMDBDFo333z+ztPBVekqf7jyMNacYIYP4XE5uHarH8bUrfk+FOXSky2/sjN7x8uxhseWsCo/IZgUOKQuCiR6PO8YMGQt999Z5NFWliSbtZ9dr5uiocBdlHDdHYtFyiYy1EiyuL7/Hz/BkhyT0cLGA0EdxlqgILXNyxcz+5F99ck9tM7z3UuZihEFsAPEZjte/4opta9ofp47vBYq25TCW9ON0TACUmVuHO9JQ8jLjsWlZTnjsYFkUrzPle+t1zSAw6kNNvQr0mw1tmKo8sjqj9YJDyBgZKzg+WXZW7W8ghrLe+T8j2SVKATXcBWBZbJws5WwadW4buWDbNvVNfPUnWgcXUIYkQ6quMQA=

	CA table (Basic Authentication)	Date: 09/01/20 13:40:55 CDT Client: 10.1.10.194 Category: EST Client ID: EST User Event: Processed EST simpleenroll request: Request ID: 412B736D737223BE6B34CB49B07D772ECF560B0C; Certificate: (Serial: 5B6F580000000000000000000000000000000008; Subject: CN=EST User, O=ISC, C=US); Signer: (Serial: 3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US); Client: EST User; EST Request: MIIDdDCCAdwCAQAwIDELMAkGA1UEBhMCVVMxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzls+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGgDzANBgkqhkiG9w0BCQ4xADANBgkqhkiG9w0BAQwFAAOCAYEAI9XAor3MpQh2VC48nauw7EDJEjfUbhQZx90YQT7pYTLddOOT9BGY8LED0JcTM/2sfdjX9hEwIdX9qHWRUs0h/5OtQvnz6BixYViMFgA1BqLIH9qtiNvdvQNz9D476+qbFGmSqxcfirBsxqDgygZK1VDY/ajKUv/ZZiGmWO6Zdj7pDobkPNIhYTFiuhORl08tNJjRM1fuO7AiCUDuID0joXcVjdgztxAI0CAZJfsFA82EnVUsM5I76OnXslbpNT03QQan8e7m4U5oR/53LPN/jJ4tr9wpuJs7CLiH1qWeffTsMyJwcelSasb7/hMyWTM0lGOcAUxbLtUD2cQVC+WzO0AY5Jh7RviBcPluSK+S1dNBHYD2DwmDpwhFYU/u5Mit/s1rr/lLXtsX+hsSsm/8zDEM+hFgWK5OP5Qm3ufGwvUvCr/Hf9PTf/NpVVt14FY1remQptrDYm6jTM+R/xC8KVRBNe652kJ29m8+D2EZhZV/zNnbaqduTe6waOwOUWjO; EST Response (200): MIIEbwYJKoZIhvcNAQcCoIIEYDCCBFwCAQExADALBgkqhkiG9w0BBwGgggREMIIEQDCCAqigAwIBAgIUW29YAAAAAAAAAAAAAAAAAAAAAAAwDQYJKoZIhvcNAQEMBQAwQjELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lTQzElMCMGA1UEAxMcQ2VydEFnZW50IDcuMC45IFJvb3QgQ0EgRENCNzAeFw0yMDA5MDExODQwNTVaFw0yNTA5MDExNDA0NDVaMC4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJU0MxETAPBgNVBAMTCEVTVCBVc2VyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuFwjjcODITvtcczCoG1BTA7dOH1LfAG+/wodCxJzZ0UaClySpQihlnNJhvhzyy54meFIsjqQisSLhAaJineTd/Yv++jAsb7Lg4Uw+o3NMo+1DYarXQ20lQ3QIE7Ae72u/pY3siJhDrPX+qVTeNzJ7a3UEzIeEYyxS78sGD/xjN/mmPNhkWr+0Mdb/+MeOG2UGDSO3u9gdRy0YTq+gKvf0pd3+sOlp3rjIqCE5E/WYSOMw3wQWjJ9FFKJ4Z6TK304xpmkKqTvDrCJM7nw02luJ/5biuMMW/X+k/izhcGnu3ukvPEYOdvdbgkPMqwZsFqTWhX3pGFEFUH90b9bwbC92cpXX6Rrwh8HTo8S4OmOYbyzVL2bISL+deYFEytoaBO+JxnGjLi1QPGtBs9RtkSOv6I/K1GuRbwJvxM8E5Z0+773FInlurMX42a1soqIJWbEcdQj6h5yiqlBOaA8pBpuSj4tERfqzls+HpLW4zlUyJB34BtLRwODYgKeMs/OFYodAgMBAAGjQjBAMB0GA1UdDgQWBBTTI9rktiax6I8u00yRFulurpck4jAfBgNVHSMEGDAWgBTL+uBdXvGZxiRh5V2eLRzg/2VauzANBgkqhkiG9w0BAQwFAAOCAYEAYrAgpVasq0ELgeLdcWUFTD8+9ab3HXID54BoT7A+WLEUuHO6q9hKBG/x98MmjqijuVymdx507ktHGYXEFKV4FCv2fS9QKBaRPhJccSp1nYRWr4zERiH7s4zRy5xhtJG6Ebq+xaRWJHUWf3gmC4G7iaMz1dnMD/Yt0p7Vozy7tftsMH727chporjQpxpd37RvVdMoouRq9I5RolEQy0pxhq6oSzR7ksFWEviuVwfJAFB3tVGH/6MddUwMjBGUmA2eWF+sOVVhX529tGFpQLcrZoHknKiBc5xkBWpb3dKg5B3kGlgXMkqliuGUoWNSeyTac0WhaVcIfJjokG+tr7/XgmJZcHky7gkI6vxCbcYjoNmKRPBG83wRknWqwIziKZuodkJi/pko/GoVs3UUKn9Aq9bt+8PeCPCBG/vC8V6TZx9gjmVt8afDp0uK7RO087jmVQPYJ8CMstbV7RqnCf17dmBbYoYSPfa881cvJcJdIbp7f2JzdpO560OydkwmdRFVMQA=
FMT_SMR.2	Admin table (Modified ACL user in Admin Site, and CA account)	Date: 09/01/20 14:01:54 CDT Client: 10.1.10.194 Category: ACL Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Added to Admin ACL; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: Admin

		Date: 09/01/20 14:07:02 CDT Client: 10.1.10.194 Category: ACL Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Updated permission in Admin ACL; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: (Admin) -> (Audit)
		Date: 09/01/20 14:08:55 CDT Client: 10.1.10.194 Category: ACL Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Removed from Admin ACL; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: Audit
		Date: 09/01/20 14:11:14 CDT Client: 10.1.10.194 Category: CA account Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Added to CA ACL: ca7; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: Admin
		Date: 09/01/20 14:12:04 CDT Client: 10.1.10.194 Category: CA account Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Updated permission in CA ACL: ca7; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN=CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: (Admin) -> (Audit)
		Date: 09/01/20 14:13:15 CDT Client: 10.1.10.194 Category: CA account Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Removed from CA ACL: ca7; Serial: 0x2ECG340000000000000000000000000000000A; Subject: CN=New User, O=ISC, C=US; Issuer: CN= CertAgent 7.0.9 Root CA DCB7, O=ISC, C=US; Permission: Audit
FPT_FLS.1	Admin table (ISC CDK failure)	Date: 09/01/20 15:00:11 CDT Client: [system] Category: system Client ID: (n/a) Event: Fatal error; Fatal error occurred at getVersionInfo. CertAgent will be shut down. Error: CDK is in error state
	Admin table (Integrity failure on Trust Anchor list)	Date: 09/01/20 15:05:12 CDT Client: [system] Category: system Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Fatal error; Fatal error occurred at ccPathValidationIfEnabled. CertAgent will be shut down. Error: Path validation failed. Cannot verify the integrity of the Trust Anchor database; Signature failure

	Admin table (Integrity failure on ACL)	Date: 09/01/20 15:26:32 CDT Client: [system] Category: system Client ID: (n/a) Event: Fatal error; Fatal error occurred at caGetAuthCAComboTag. CertAgent will be shut down. Error: Cannot verify the integrity of the ACL database; Signature failure
FPT_KST_EXT.2	Admin table (Failed to login to CA account)	Date: 09/01/20 16:52:41 CDT Client: 10.1.10.194 Category: CA account Client ID: CN=New User, O=ISC, C=US Event: Cannot login to the CA Account site; error: Unauthorized
	Admin table (Failed to login to Admin site)	Date: 09/01/20 16:53:52 CDT Client: 10.1.10.194 Category: login Client ID:CN=New User, O=ISC, C=US Event: Login failed; error: Unauthorized
	CA table (Failed to access RAMI)	Date: 09/01/20 16:54:21 CDT Client: 10.1.10.194 Category: RAMI Client ID: CN=New User, O=ISC, C=US Event: Cannot process RAMI request; error: You are not an authorized user
FPT_RCV.1	Admin table	Date: 09/01/20 15:10:22 CDT Client: [system] Category: system Client ID: (n/a) Event: Resumed regular operations after fatal error occurred on 09/01/20 15:05:12 CDT at ccPathValidationIfEnabled; Error: Path validation failed. Cannot verify the integrity of the Trust Anchor database; Signature failure
FPT_TUD_EXT.1	Admin table	Date: 09/01/20 16:58:22 CDT Client: [system] Category: system Client ID: Update Tool Event: Running update script version: 7.0.9.1
FPT_TST_EXT.2	Admin table (Ran tests on demand by admin)	Date: 09/01/20 17:01:41 CDT Client: 10.1.10.194 Category: NIAP Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Ran integrity test on the Trust Anchor database: passed
		Date: 09/01/20 17:02:11 CDT Client: 10.1.10.194 Category: NIAP Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Ran integrity test on the ACL database: passed
	Admin table (Ran tests on startup)	Date: 09/01/20 17:10:30 CDT Client: [system] Category: NIAP Client ID: (n/a) Event: Ran integrity test on the Trust Anchor database: passed
		Date: 09/01/20 17:10:30 CDT Client: [system] Category: NIAP Client ID: (n/a) Event: Ran integrity test on the ACL database: passed

	Admin table (Ran test on startup; integrity violation)	Date: 09/01/20 17:15:30 CDT Client: [system] Category: NIAP Client ID: (n/a) Event: Ran integrity test on the Trust Anchor database: failed; error: Cannot verify the integrity of the Trust Anchor database; Signature failure
		Date: 09/01/20 17:18:13 CDT Client: [system] Category: NIAP Client ID: (n/a) Event: Ran integrity test on the ACL database: failed; error: Cannot verify the integrity of the ACL database; Signature failure
FTA_SSL.4	Admin table	Date: 09/01/20 10:26:24 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Logged out
	CA table	Date: 09/01/20 10:28:12 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Logged out
FTA_SSL.3	Admin table	Date: 09/01/20 11:12:43 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US Event: Logged out due to session timeout
	CA table	Date: 09/01/20 11:15:54 CDT Client: 10.1.10.194 Category: login Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Logged out due to session timeout
FTP_TRP.1	Admin table (Privileged users connected to CA site, Admin site, RAMI, DBAccess, or subscribers connected to EST or self-revocation services)	Date: 09/01/20 10:11:22 CDT Client: 10.1.10.194 Category: TLS session Client ID: CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Established trusted channel
		Date: 09/01/20 10:13:49 CDT Client: 10.1.10.194 Category: TLS session Client ID:CN=CertAgent 7.0.9 Auditor, O=ISC, C=US Event: Terminated trusted channel
	Admin table (Subscribers or replying parties connected to Public Site)	Date: 09/01/20 10:43:51 CDT Client: 10.1.10.194 Category: TLS session Client ID: (n/a) Event: Established trusted channel
		Date: 09/01/20 10:43:51 CDT Client: 10.1.10.194 Category: TLS session Client ID: (n/a) Event: Terminated trusted channel

	Admin table (Failures of the trusted path functions to all interfaces)	Date: 09/01/20 09:36:27 CDT Client: 10.1.10.194 Category: TLS session Client ID:(n/a) Event: Cannot establish trusted channel; error: Client requested protocol TLSv1.1 is not enabled or supported in server context
FTP_ITC.1	Admin table (RA connected to RAMI or Audit Server connected to DBAccess service)	Date: 09/01/20 09:38:25 CDT Client: 10.1.10.194 Category: TLS session Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Established trusted channel
		Date: 09/01/20 09:38:26 CDT Client: 10.1.10.194 Category: TLS session Client ID: CN=CertAgent 7.0.9 CA Operations Staff, O=ISC, C=US Event: Terminated trusted channel
		Date: 09/01/20 09:40:19 CDT Client: 10.1.10.194 Category: TLS session Client ID: (n/a) Event: Cannot establish trusted channel; error: Client requested protocol TLSv1.1 is not enabled or supported in server context

TABLE 43 SAMPLE DATABASE AUDIT TRAIL

5.2.2.2.2 Local Server Log File

TOE creates a local server log file located at:

```
/usr/local/certagent7/conf/server.log                    (CentOS)
C:\Program Files\CertAgent7\conf\server.log               (Windows)
```

The description of each available field, the format of the field, and the data displayed in the log file are given in the following table. Each field is delimited by a space, and each record is delimited by a new line.

Field	Description
Date and time	Date and Time Start and end with a pipe character Format: |<MM/DD/YYYY> <HH:MM:SS ZZZ>| E.g. |09/01/2020 15:34:31 CDT|
Event level	Event level: INFO or ERROR Format: [INFO] or [ERROR]
Client	(Optional) Client IP address or local command line program Format: [IP: <IP Address>] or [IP: CACLI]
Client ID	(Optional) The identity of the client in string: Subject DN of an authorized user's certificate or CACLI Format: [Client ID: <client ID>]
Event	Recorded events in string

TABLE 44 SERVER LOG FILE FIELD AND DESCRIPTION

Sample formats:

```
|<MM/DD/YYYY> <HH:MM:SS ZZZ>|[INFO or ERROR] <event>
|<MM/DD/YYYY> <HH:MM:SS ZZZ>|[INFO or ERROR] [IP: <IP Address or CACLI>]
 [Client ID: <client ID>] <event>
```

The following events will be recorded in the log file:

- Starting/Stopping/started/stopped CertAgent services
- Starting/Stopping/started/stopped Tomcat services
- Fatal errors that caused the TOE to shut down

The TOE stores the FPT_FLS.1 auditable events in the server log file. The failure types and the sample events are given in the following table:

Failure Type	Sample Log
ISC CDK failure	|09/01/2020 15:34:31 CDT|[ERROR] [IP: CACLI] [Client ID: CACLI] Fatal error occurred at getVersionInfo. CertAgent will be shut down. Error: CDK is in error state
Integrity failure on Trust Anchor list	|09/01/2020 12:18:12 CDT|[ERROR] [Client ID: CN=CertAgent 7.0.9 Administrator, O=ISC, C=US] Fatal error occurred at ccPathValidationIfEnabled. CertAgent will be shut down. Error: Path validation failed. Cannot verify the integrity of the Trust Anchor database; Signature failure
Integrity failure on ACL	|09/01/2020 12:28:12 CDT|[ERROR] Fatal error occurred at caGetAuthCAComboTag. CertAgent will be shut down. Error: Cannot verify the integrity of the ACL database; Signature failure
Database inaccessible	|09/01/2020 13:47:11 CDT|[ERROR] [IP: 10.1.10.194] Fatal error occurred at ocspProcessRequest. CertAgent will be shut down. Error: Database error: ERROR: could not extend file "base/16389/16509": No space left on device. Hint: Check free disk space.

TABLE 45 SAMPLE SERVER LOG FILE

NOTE: Above failure events, except the database inaccessible one, are also recorded in the Audit Table.

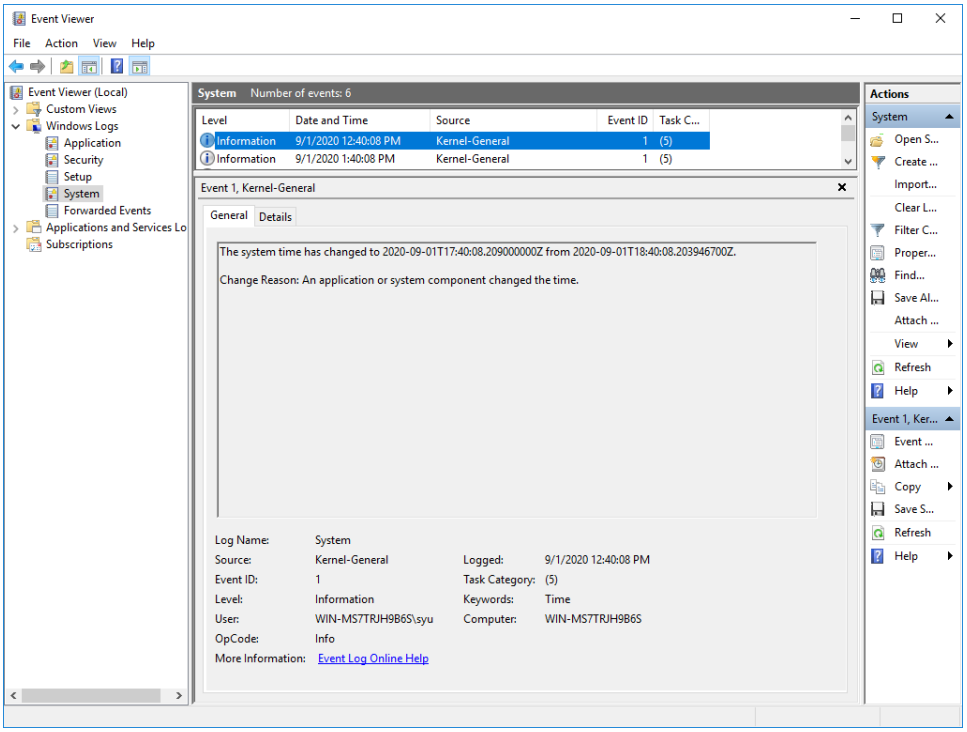
5.2.2.2.3 Operating System Logs

FPT_STM.1 is the only SFR records the event to the Operational Environment.

To view the time changed log on Windows 2016:

1. Login to the Windows system as an OE Auditor.
2. Right click on the Windows icon on the toolbar and select Event Viewer.
3. In the left panel, select Windows Logs, System.
4. From the Source column, locate the Kernel-General item containing the time change entry.

   Sample log:



To view the time changed log on CentOS 7.8:

NOTE: In order to record the time changed event, audit service must be configured. For details, see section *5.1.8 Configuring Audit Setting in CentOS*.

1. Login to the CentOS system as OE Auditor.
2. Open the audit file: /etc/audit/audit.log.
3. Locate the time changed event by searching for `key="time-change"` where `time-change` is the name defined in audit configuration file.

   Sample log:

   ```
   type=SYSCALL msg=audit(1599070992.080:1872): arch=c000003e syscall=227
   success=yes exit=0 a0=0 a1=7ffd1c7130c0 a2=0 a3=7ffd1c712aa0 items=0
   ppid=5927 pid=5929 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
   sgid=0 fsgid=0 tty=pts1 ses=11 comm="date" exe="/usr/bin/date"
   subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="time-
   change"
   ```

   Use a timestamp conversion tool (e.g., www.epochconverter.com) to convert the timestamp to a human readable date. The "1599070992.080" value represents the date and time (Wednesday, September 2, 2020 6:23:12.080 PM GMT) when the changing system time occurred.

4. Locate the new time event by searching for `exe="/sbin/hwclock"`.

   Sample log:

```
type=USYS_CONFIG msg=audit(1599069604.499:1875): pid=5939 uid=0 auid=0
ses=11 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=change-system-time exe="/usr/sbin/hwclock"
hostname=localhost.localdomain addr=? terminal=pts/1 res=success'
```

The "1599069604.499" value represents the new time (Wednesday, September 2, 2020 6:00:04.499 PM GMT) that the clock changed to.

5.2.3 FAU_STG.4 Prevention of Audit Data Loss

Full audit trail means no audit records can be written to the audit trail table that happens when the hard disk is full.

If the database is inaccessible or the audit trail becomes full (or the disc storage is exhausted), the TOE will display a fatal error message on any attempt to access any of the TOE interfaces, including web interfaces, RAMI, DBAccess, etc. The TOE will record the error message to the local server log file indicating the database error and then shut itself down.

Sample of the error message if the disk is full:

```
|09/01/2020 13:47:11 CDT|[ERROR] [IP: 10.1.10.194] Fatal error occurred at
ocspProcessRequest. CertAgent will be shut down. Error: Database error: ERROR:
could not extend file "base/16389/16509": No space left on device Hint: Check
free disk space.
```

The TOE does not allow an auditor (or anyone else) to perform any actions after shutting down. Auditors trying to access the web interface will receive "Unable to connect" error message from the browser. This error message indicates the TOE is not running, and a fatal error may have occurred. An audit trail cannot be written to, and storage capacity has been reached could be the cause. Auditors should contact the Administrators of the OS platform to locate the fatal error from the local server log file. If the error is due to full disk space, Administrators of the OS platform should allocate more disk spaces to the existing one or migrate the database to a new hard disk with a larger capacity. Once the issue has been fixed, Administrators should follow the steps in section *4.1.1 Managing the TOE Service* to start the TOE.

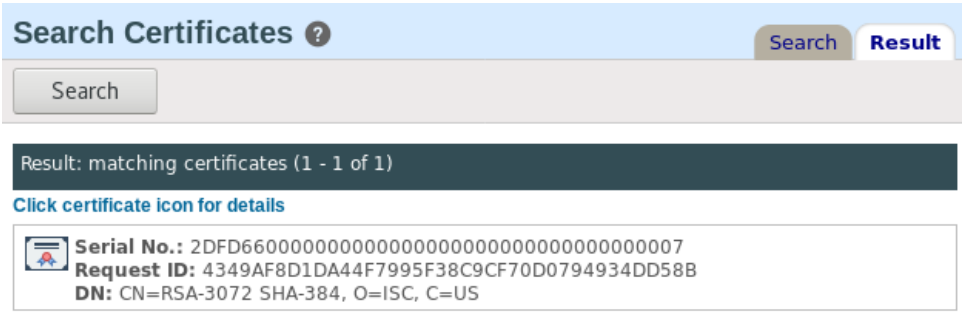
5.2.4 FAU_SCR_EXT.1 Certificate Repository Review

The TOE's web interface allows Auditors to search for certificates by subject name or serial number, and the search results can include the certificate request ID, which can then be used to search the audit trail for any events related to that certificate.

To search for certificates matching certain criteria in the certificate repository:

1. Follow the steps in *section 4.5.5.1 Searching Certificates* and select your Auditor certificate.
2. To search for all valid certificates and return serial number, request ID, and subject DN information, keep the default settings (Status: Valid, include the serial number and DN in the report), and check the **Request ID** checkbox.

3. Click **Search**. Matching certificates will be returned.
   For example:



To search for audit records matching serial number or subject DN:

1. Follow steps in section *4.5.2 Searching the Audit Trail*.
2. In the Basic section, check the Event matches box.
3. To search for a particular serial number, enter "*Serial: <serial>*" and click **Search**.
   For example:

```
*Serial: 2DFD660000000000000000000000000000000007*
```

   The audit entries associated with this serial number will appear in the result.
   For example:

   Event:

```
Processed request: Request ID: 4349AF8D1DA44F7995F38C9CF70D0794934DD58B;
Certificate: (Serial: 2DFD660000000000000000000000000000000007; Subject:
CN=RSA-3072 SHA-384, O=ISC, C=US); Signer: (Serial:
3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root
CA DCB7, O=ISC, C=US)
```

4. To search for a particular subject DN, enter "*Subject: <subject DN>*" and click Search.
   For example:

```
*Subject: CN=RSA-3072 SHA-384, O=ISC, C=US*
```

   The audit entries associated with this serial number will appear in the result.
   For example:

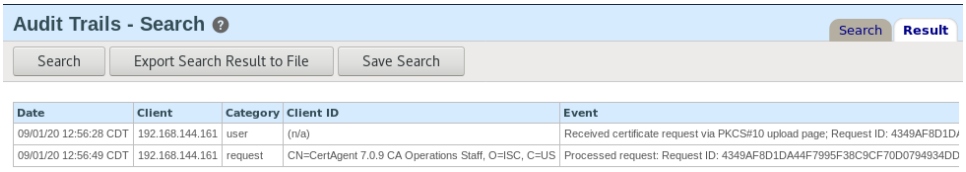
Event:

```
Processed request: Request ID: 4349AF8D1DA44F7995F38C9CF70D0794934DD58B;
Certificate: (Serial: 2DFD66000000000000000000000000000000000007; Subject:
CN=RSA-3072 SHA-384, O=ISC, C=US); Signer: (Serial:
3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root
CA DCB7, O=ISC, C=US)
```

5. To search for a particular request ID, enter "*Request ID: <request ID>*" and click Search. For example:

```
*Request ID: 4349AF8D1DA44F7995F38C9CF70D0794934DD58B*
```

The audit entries associated with this request ID will appear in the result.



Events:

```
Received certificate request via PKCS#10 upload page; Request ID:
4349AF8D1DA44F7995F38C9CF70D0794934DD58B
```

```
Processed request: Request ID: 4349AF8D1DA44F7995F38C9CF70D0794934DD58B;
Certificate: (Serial: 2DFD66000000000000000000000000000000000007; Subject:
CN=RSA-3072 SHA-384, O=ISC, C=US); Signer: (Serial:
3CE4F10000000000000000000000000000000001; Subject: CN=CertAgent 7.0.9 Root
CA DCB7, O=ISC, C=US)
```

5.2.5 FAU_SEL.1 Selective Audit

Administrators of the Admin Site can select the set of events to be audited to the Admin's Audit table based on the event type. Below table describes each event type supported by the Admin Site Audit Trail.

By default, all types of auditable events are selected in the Audit Trail Configuration page, and all auditable events will be recorded in the Audit table. To configure the auditable events, follow the steps in section *4.4.4 Configuring Audit Trail Settings.*

NOTE: Each event type is configurable. None of the events in the Admin Audit Trail are always recorded regardless of the selection criteria.

Type	Description
ACL	Updated Admin ACL
Audit	Updated audit trail configuration, Audit function started, or updated saved audit search
CA account	Created/Enabled/Disabled CA accounts, updated CA ACL, or invalid access to CA Account via CA Site, RAMI, DBAcess, and EST
Credential	Generated/Updated System credentials
Database	Updated database configuration
DBAccess	DBAccess requests
Email	Updated email configuration, or sent error alert email
Job	Added/Removed/Updated/Ran/Locked/Unlocked jobs
Login	Succeeded/Failed to login or logout
NIAP	Updated NIAP settings, started integrity test on startup, ran integrity test, integrity test result, signed trust anchor/ACL table when integrity setting changed from disabled to enabled, updated trust anchor/CRL for path validation
PIN	Entered system PIN
System	Operated mode of CertAgent, started/stopped Tomcat, stopped CertAgent, fatal error, resumed regular operations after a fatal error, or events triggered from installer or update tool
TLS session	Succeeded/Failed to establish trust channel or terminated trust channel
Dhuma	Managed Dhuma accounts, updated account configurations, or processed OCSP requests

TABLE 46 ADMIN SITE AUDIT TRAIL EVENT TYPE AND DESCRIPTION

Audit records for the CA account are always recorded to the CA's Audit table regardless of the selection criteria configured in the Admin Site. Below table describes each event type supported by the CA Account Audit Trail.

Type	Description
request	Rejected/processed/reconsidered requests, assigned a request to other profile, or failed to link a certificate with a request
certificate	Changed certificate status, assigned a certificate to other profile, ran a process to check for expired certificates, changed the status of affected certificates from pending revocation to revoked after issuing a CRL, or imported/exported certificate via CACLI
CRL	Issued CRLs, imported a CRL via CACLI, updated CRL Number extension via CACLI after importing a CRL, or started/stopped automated CRL issuance
OCSP	Processed OCSP requests
user	Submitted certificate requests, retrieved certificates, or processed self-service certificate revocation requests
login	Succeeded/Failed to login or logout
credential	Generated new CA credential, installed CA certificate into HSM, assigned credential to CA account, submitted certificate request to a superior CA, or decrypted encrypted password using System credential
RAMI	Succeeded/Failed to process RAMI requests
DBAccess	Succeeded/Failed to process DBAccess requests
configuration	Updated account configuration
EST	Succeeded/Failed to process EST requests

TABLE 47 CA ACCOUNT AUDIT TRAIL EVENT TYPE AND DESCRIPTION

Audit records written to a local server log file are always recorded.

5.2.6 FAU_STG_EXT.1 External Audit Trail Storage

The TSF maintains audit data locally in the environmental database and file system, which are both located on the same host system as the TOE. The TOE communicates with the database using the database access URL, user, and password via the Java JDBC API. When an audit event is generated, it is simultaneously sent to the database.

During the installation, the local administrator will be prompted for the database access information. For details, see the installation sections 3.2.1 Windows and 3.2.2 CentOS.

There is no configuration in the evaluated databases (PostgreSQL and HyperSQL) to set the size of the database tables. The size of the audit storage is limited by the disc space available on the TOE platform.

Audit trail data may be transferred to an external IT entity by having that entity use the DBAccess REST API. This connection is client-authenticated and encrypted using TLS/HTTPS. When an audit event is generated, it does not send to the external entity automatically. The external IT entity is expected to initiate the connection to the TOE and poll the TOE periodically to obtain updated audit entries. For details on this service, see section *4.8 Using Database Access Service*.

5.3 Communications (FCO)

5.3.1 FCO_NRO_EXT.2 Certificate-based proof of origin

Any certificate request submitted to the TOE must have a valid proof of origin regardless of how it is submitted (upload, EST, etc.). Except for requests submitted through RAMI, the TOE requires a valid digital signature covering the request by a private key matching the public key in the request. The digital signature on these requests is checked when they are submitted, and, if not valid, the request is rejected. In the case of an RA using RAMI, the RA can be responsible for proving the origin of requests it submits and such proof implied by the RA's submission of the request. Thus the TOE supports unsigned certificate requests through RAMI only. The TOE always verifies the digital signature of the certificate requests, which is not configurable. However, the hash algorithm used to sign the certificates is configurable. For details, see 'Message Digest' option in section *4.5.7.4.1 Properties*.

The TOE generates CRLs and provides a built-in OCSP responder for issuers hosted by the TOE. CRLs and OCSP responses are digitally signed. The signature provides proof of origin. The hash algorithm used to sign CRLs and OCSP responses is configurable. For details, see 'Message Digest' option in section *4.5.7.5 Managing CRL Issuance* and 'Hash Algorithm' option in section *4.5.7.6 Managing OCSP Responder Settings*.

The TOE also provides an OCSP responder for external issuers. The hash algorithm used to sign OCSP responses is configurable. For details, see 'Hash Algorithm' option in section *4.4.10.2.4 Configuring OCSP Response Settings*.

The TOE supports EST's simple enrollment as defined in FIA_ESTS_EXT.1. Subscribers connect to the TOE using EST basic authentication or client authentication via HTTP/TLS. Requests received via EST must be digitally signed. The TOE's EST responses contain the issued and signed certificate matching the request. For details on configuring EST, see sections *4.5.7.1.3 EST (Enrollment over Secure Transport)* and *4.5.7.9.2 EST (Enrollment over Secure Transport) Users*.

Simple EST doesn't support revocation. The TOE allows a subscriber to request their certificate be revoked using a HTTPS/TLS client authenticated web page. Once the subscriber successfully authenticates to the TOE, using a certificate, the TOE displays a list of certificates issued by the same issuer DN and with the same subject DN as the certificate used to authenticate. The subscriber can then select one or more certificates from that list and revoke them. For details on enabling self-service revocation, see section *4.5.7.9.1 Certificate Revocation*. For details on submitting revocation requests, see section *4.6.6 Using Self-service Revocation*.

5.4 Cryptographic Support (FCS)

The TOE includes its own cryptographic module (the ISC CDK) and also uses an external component (the PKCS#11 Cryptographic Module) for cryptographic functions. The easiest summary is that the PKCS#11 Cryptographic module performs all sensitive private key operations, and the TOE uses the ISC CDK for everything else. Both the ISC CDK and the PKCS#11 Cryptographic Module in the evaluated configuration are FIPS 140-2 validated.

5.4.1 FCS_CKM.1 Cryptographic Key Generation

The TOE installer uses the PKCS#11 Cryptographic Module to create credentials for TLS/HTTPS server authentication, an issuer, and the System. It uses the ISC CDK to generate the initial set of authentication credentials. The key type and size of these credentials is either RSA-3072 or US-P-384 and is configurable during the installation. These credentials should be considered temporary and only used to facilitate initial system setup; they should be replaced with properly issued credentials before making the system operational.

The TOE uses the PKCS#11 Cryptographic Module to generate RSA or ECC System keys to be used when encrypting sensitive data before storing it in the environmental database and signing the trust anchor list and ACLs to ensure data integrity. The allowed key sizes and types are: RSA-3072, RSA-4096, RSA-8192, US-P-256, US-P-384, and US-P-521. To update the system credential, see section *4.4.8 Managing System Credential* for details.

The TOE uses the PKCS#11 Cryptographic Module to generate RSA or ECC Issuer keys for certificate issuance, CRL signing, and OCSP response signing. The allowed key sizes and types are: RSA-3072, RSA-4096, RSA-8192, US-P-256, US-P-384, and US-P-521. For details, follow the steps in *section 4.5.3 Managing CA Credentials* to specify the desired key type and size.

The TOE uses the PKCS#11 Cryptographic Module to generate RSA or ECC keys for HTTPS/TLS server authentication. To configure a new TLS credential with a different key size, see section *4.11 Replacing TLS Credentials.*

The TOE uses the PKCS#11 Cryptographic Module to generate RSA or ECC delegated OCSP signer keys for OCSP response signing. The allowed key sizes and types are: RSA-3072, RSA-4096, RSA-8192, US-P-256, US-P-384, and US-P-521. To configure a new delegated OCSP signer for an issuer hosted by the TOE, see section *4.5.7.6.1.2 Generating a New Delegated Signer Credential*. To configure a new delegated OCSP signer for an external issuer, see section *4.4.10.2.1 Generating a New Delegated OCSP Signer Credential*.

5.4.2 FCS_CKM.2 Cryptographic Key Establishment

The TOE uses the ISC CDK to generate an ephemeral asymmetric cryptographic key for key establishment as a recipient during TLS/HTTPS session establishment and as a sender and recipient when the System credential is an ECC key pair.

For TLS ECDHE Key, the TOE uses the ISC CDK to generate these keys as part of the HTTPS/TLS negotiation. The key type is negotiated during session setup and is one of the NIST curves P-256, P-384, or P-521. These curves have been configured upon installation automatically. These settings are specified in the `CA_OPTS` variable (`-Djdk.tls.namedGroups=secp256r1,secp384r1,secp521r1`) in the TOE's configuration file (`<ca home>/setenv.sh or setenv.bat`). To configure the allowed curves, update the `CA_OPTS` variable, and restart the TOE.

The TOE installer creates an RSA-3072/SHA-384 or an ECDSA P-384/SHA-384 credential for the HTTPS/TLS server using the PKCS#11 Cryptographic Module. To configure a new TLS credential with a different key size, see section *4.11 Replacing TLS Credentials.*

The TOE uses the ISC CDK to generate an ephemeral ECDH key pair when encrypting sensitive data using CMS when the System credential is an ECC key pair. The TOE installer creates an RSA-3072/SHA-384 or an ECDSA P-384/SHA-384 System credential. This system credential can be updated after installation. The allowed key sizes and types are: RSA-3072, RSA-4096, RSA-8192, US-P-256, US-P-384, and US-P-521. For details on updating the System credentials, see section *4.4.8 Managing System Credential*.

NOTE: The TOE supports RSA-4096 and larger key sizes but they were not tested for use in the evaluated configuration.

5.4.3 FCS_CKM_EXT.4 Cryptographic Key Destruction

The key destruction functionality is not configurable.

By default, the TSF destroys all cryptographic keys (CMS DEK and TLS ECDHE) and sensitive data (PKCS#11 cryptographic PIN, database passwords, and EST subscriber passwords) when no longer needed.

All other keys on which the TOE is dependent are managed and destroyed by the environmental PKCS#11 Cryptographic Module. The TOE's own key destruction process does not fail as it simply clearing memory allocated by the environmental Operation System using APIs provided by the same.

5.4.4 FCS_COP.1(1) Cryptographic Operation (AES Encryption/Decryption)

By default, the TOE uses the ISC CDK to perform AES-CBC or AES-GCM encryption/decryption with 256-bit keys during TLS/HTTPS negotiation and when storing/retrieving sensitive data in the database. The encryption algorithm, mode, and key size are automatically configured upon installation.

5.4.5 FCS_COP.1(2) Cryptographic Operation (Cryptographic Signature)

By default, the TOE supports both RSA and ECDSA algorithms. The algorithm and key size for the specified operations are determined solely by the key type and size of the public/private key that is performing the operation. For RSA key pairs, the RSA algorithm will be used. For ECC key pairs, the ECDSA algorithm will be used. To change the key type/size used, you must change the credential.

The System, Issuer, TLS, Authentication, and delegated OCSP signer credentials generated during the installation are either RSA-3072/SHA-384 or ECDSA P-384/SHA-384. However, these credentials can be changed post-installation. To change the Issuer credential that signs certificates, CRLs, and OCSP responses, see *section 4.5.3 Managing CA Credentials.* To change the System credential that encrypts sensitive data and signs Trust Anchor and CRL databases, see section *4.4.8 Managing System Credential.* To change the TLS credential, see section *4.11 Replacing TLS Credentials.* To change the delegated OCSP signer credential that signs OCSP responses, see section *4.5.7.6.1.2 Generating a New Delegated Signer Credential and* section *4.4.10.2.1 Generating a New Delegated OCSP Signer Credential*.

The TOE uses the PKCS#11 Cryptographic Module to perform cryptographic signatures for certificate signing, CRL signing, OCSP response signing, and signatures requiring the TLS/HTTPS server certificate. The Web Browser performs cryptographic signatures for identifying the user authenticating to the TOE. The TOE itself performs signature verification operations (of TLS client certificates, certificates on ACLs, and software update packages) and signs the initial authentication certificate requests.

5.4.6 FCS_COP.1(3) Cryptographic Operation (Cryptographic Hashing)

The TOE uses the ISC CDK to perform cryptographic hashing as follows:

- When establishing a TLS/HTTPS connection
  - Supports the TLS 1.2 PRF with SHA-256, SHA-384, and corresponding message digest sizes 256-, 384-bits
  - Supports SHA-1, SHA-256, SHA-384, and SHA-512 for signature validation as required by TLS 1.2
  - Supports SHA-1, SHA-256, SHA-384, SHA-512 for signature generation as required by TLS 1.2

- When digitally signing the Trust Anchor and ACL database tables for integrity protection, SHA-384 is used (which is not configurable).
- When creating certificates, certificate requests, and CRLs, SHA-384, and SHA-512 and message digest size 384 and 512 are supported.

  For details on configuring the message digest for certificates, see sections *4.5.3.1 Generating Credential for a Root CA* and *4.5.7.4.1 Properties*.

  For details on configuring the message digest for certificate requests, see section *4.5.3.2 Generating Credential for Subordinate CA*.

  For details on configuring the message digest for CRLs, see section *4.5.7.5 Managing CRL Issuance*.
- When creating OCSP responses, SHA-1, SHA-256, SHA-384, SHA-512, and message digest sizes 160, 256, 384, and 512 are supported. For details on configuring the message digest, see section *4.5.7.6 Managing OCSP Responder Settings* for internal issuers and section *4.4.10.2.4 Configuring OCSP Response Settings* for external issuers.
- When verifying certificates, CRLs, and certificate requests, SHA-1, SHA-256, SHA-384, SHA-512, and message digest sizes 160, 256, 384, and 512 are supported.

There is no option in the TOE to disable deprecated algorithms.

5.4.7 FCS_COP.1(4) Cryptographic Operation (Keyed-Hash Message Authentication)

The TOE uses the ISC CDK to perform key hash message authentication as follows:

- When establishing a TLS/HTTPS connection
  - Supports the TLS 1.2 PRF (which uses HMAC-SHA-256 or HMAC-SHA-384 for parts of the computation depending on the ciphersuite) with key size 256-, 384-, 521-bits (based on the ECC key type negotiated) and output size of 256-, 384-, 512-bits (the PRF outputs 96-, 384-, 576-, and 1088-bits by repeatedly invoking the HMAC operations if necessary)
  - Supports the TLS 1.2 HMAC (which uses HMAC-SHA-1 or HMAC-SHA-384 depending on the ciphersuite) with key sizes of 160-, 384-bits and output size of 160, 384-bits
- When performing PBKDF2 for creating the EST password check values (Note: PBKDF2 is performed when a privileged user in the CA Operations Staff role creates the password or when a subscriber authenticates with the password)
  - Uses HMAC-SHA-256 with key size 120-800-bits and output size of 256-bits
- When generating random numbers
  - Uses HMAC-SHA-256 with key size 256-bits and output size of 256-bits

There is no option in the TOE to configure the key hash message authentication.

5.4.8 FCS_RBG_EXT.1 Cryptographic Random Bit Generation

The TOE uses the two cryptographic modules to generate random numbers in the following ways.

- The PKCS#11 Cryptographic Module
  - CTR_DRBG(AES-256)

- Provider: Thales Luna USB HSM
- Entropy Source: hardware-based noise source providing 384-bits of entropy

- The TOE using the ISC CDK
  - HMAC_DRBG(SHA-256)
  - Provider: ISC CDK
  - Entropy Source: third-party software-based noise source providing more than 256-bits of entropy

There is no option in the TOE to configure the RBG service.

5.4.9 FCS_TLSS_EXT.1 TLS Server Protocol

The TOE supports the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

The default, initial, TLS/HTTPS server key is RSA-3072. The TLS/HTTPS server key can be replaced with an RSA-4096, or larger or an ECC key pair if desired, but this was not tested for use in the evaluated configuration. The only supported elliptic curve parameters are NIST curves secp256r1, secp384r1, and secp521r1, also known as P-256, P-384, P-521, US-P-256, US-P-384, and US-P-521.

Only TLS 1.2 is supported in the evaluated configuration. Connections requesting SSL 2.0, SSL 3.0, TLS 1.0 or TLS 1.1 are rejected.

TLS 1.2 and the ciphersuites have been configured in Tomcat upon installation automatically. These settings are specified in the `ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA"` and `sslEnabledProtocols="TLSv1.2"` attributes of the Connector elements in the Tomcat configuration file (`<ca home>/tomcat/conf/server.xml`). No configuration is required.

5.4.10 FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication

The TOE supports the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

The default, initial, TLS/HTTPS server key is RSA-3072. The TLS/HTTPS server key can be replaced with an RSA-4096, or larger or an ECC key pair if desired, but this was not tested for use in the evaluated

configuration. TLS 1.2 and the ciphersuites have been configured in Tomcat upon installation automatically. These settings are specified in the `ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA"` and `sslEnabledProtocols="TLSv1.2"` attributes of the Connector elements in the Tomcat configuration file (`<ca home>/tomcat/conf/server.xml`). No configuration is required.

Only TLS 1.2 is supported in the evaluated configuration. Connections requesting SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0 or TLS 1.1 are rejected.

The only supported elliptic curve parameters are NIST curves secp256r1, secp384r1, and secp521r1 also known as P-256, P-384, P-521, US-P-256, US-P-384, and US-P-521.

Mutual authentication using a valid X.509 certificate is required to access the Admin Site and CA Account Site. For the certificate used to authenticate to these sites:

- it must be an end entity certificate
- it must not be expired
- it must have the Client Authentication purpose set in the extended key usage extension
- it must pass the path validation
- its certificate path must terminate with a certificate in the trust anchor database and Tomcat's trust keystore
- all CA certificates in the path must contain a basic constraints extension asserting the cA flag
- its status must be valid by checking the revocation status using a CRL
- the subject DN of the certificate must match the DN filter (default to "*")

Upon TOE installation, client and root credentials have been created with certificates fulfilling the above requirements. The TOE has been configured with the root certificate and CRL installed in the trust anchor database and CRL store respectively. Tomcat has been configured with the root certificate installed in the trust keystore and to open the TLS port with mutual authentication for Admin and CA sites. No configuration is required.

If the client certificate cannot fulfill any of the above requirements, the certificate is invalid, and the TOE will not establish a trusted channel. No configuration is required.

The TOE supports filtering client certificates by their distinguished name (DN) to allow an administrator to restrict access to only matching certificates. If a client certificate's DN does not match the configured filter, the TOE will respond with a fatal TLS error. This filter applies to all interfaces using mutual authentication. By default, the filter is set to "*" to allow any DNs. For details on configuring the DN filter, see section *4.4.2.2.3 Client Certificate DN Filter.*

5.4.11 FCS_STG_EXT.1 Cryptographic Key Storage, FCS_COP.1(5) Cryptographic Operation (Password-Based Key Derivation Function), FCS_CKM_EXT.1(1) Symmetric Key Generation for DEKs, FCS_CKM_EXT.5 Public Key Integrity, FCS_CKM_EXT.8 Key Hierarchy Entropy

No configurable actions.

5.5 User Data Protection (FDP)

5.5.1 FDP_CER_EXT.1 Certificate Profiles

The TOE implements a certificate profile function and issues certificates consistent with the profile's configuration. A CA account can have one or more profiles which are configured by an administrator using the TOE's web interface. For details on managing the certificate profiles and their issuance settings, see sections *4.5.7.3 Managing Certificate Profiles* and *4.5.7.4 Managing Certificate Issuance.*

Any certificate request submitted to the TOE must have a valid proof of origin regardless of how it is submitted (upload, EST, etc.). Otherwise, the request will be rejected. There is no option in the TOE to configure the proof of possession setting.

Unique serial number generation is not configurable. TSF uses the database sequence to keep track of the next sequential number. Each 20-byte serial number consists of 3 leading random bytes and 17 bytes representing the next sequential number, padded with leading zeros.

5.5.2 FDP_CER_EXT.2 Certificate Request Matching

5.5.2.1 Tracing a Submitted Request to an Issued Certificate

Each certificate request is identified by a unique request ID which is linked to the issued certificate. Each certificate is identified by a unique issuer DN and serial number.

To trace a request to an issued certificate:

1. Follow the steps in *section 4.5.1 Logging in the CA Account Site* and select your CA operations staff certificate with 'certify' permission.
2. In the left panel, click **Certificate, Search**.
3. Check the **Request ID matches** checkbox, specify a request ID in the associated field, uncheck the **Status** checkbox, check the **Serial number** checkbox in the right column to include the serial number in the report, and click **Search**.
4. If a matching certificate request is found and a certificate has been issued, its serial number will be displayed in the result.
5. Click the certificate icon to open an **Advanced** function page to view the certificate's status and available actions.

To trace an issued certificate to a request:

1. Check the **Serial number matches** checkbox, specify a serial number in the associated field, uncheck the **Status** checkbox, check the **Request ID** checkbox in the right column to include the request ID in the report, and click **Search**.
2. If a matching certificate is found, its request ID, along with selected information, will be displayed.
3. Click the certificate icon to open an **Advanced** function page to view the certificate's status and available actions. Click the Request ID link to open an **Advanced** function page for the request.

5.5.3 FDP_CER_EXT.3 Certificate Issuance Approval

The TOE supports the approval of certificates issued according to a configured certificate profile through the web interface, RAMI, or EST.

RAMI and EST settings have already been configured in section *5.1 Prerequisite*.

To approve requests manually via the web interface, following the steps in section *4.5.4.3 Issuing Certificates.*

A privileged user with ‘CA Operations Staff’ role and ‘RAMI’ permission can submit a request to RAMI, specifying the profile to use. The request will be approved automatically as long as they have ‘RAMI’ permission for the requested profile.

An authenticated subscriber can submit a request to the EST interface, and the request will be approved automatically.

5.5.4 FDP_CSI_EXT.1 Certificate Status Information

The TOE provides certificate status information whose format complies with ITU-T Recommendation X.509v2 CRL, and the OCSP standard as defined by IETF RFC 6960.

By default, when certificates initially designated as 'revoked', are immediately moved to a 'revoked certificates' list, and only those with 'on hold' status can later be reinstated. If the pending revocation option is enabled, certificates initially flagged as revoked are first moved to a list of certificates 'pending revocation' from which they can be reinstated at any time prior to issuance of a CRL (in which they'll appear). Once a CRL containing them has been issued, they are moved to the revoked certificates list from which only 'on hold' certificates can be reinstated. To configure this option, see section *4.5.7.8 Managing Revocation Policy*.

Privileged users with ‘CA Operations Staff’ role and ‘revoke’ permission can approve changes to the status of a certificate via the CA Account site. For details, see section *4.5.5.3 Revoking Certificates*.

Privileged users with ‘CA Operations Staff’ role and ‘RAMI’ permission can approve changes to the status of a certificate via the RA Management Interface (RAMI). For details, see section *4.7.3 Revoking a Certificate.*

Subscribers can approve changes to their certificate's status via the self-service revocation page in the Public Site. Subscribers can only revoke and are only presented with certificates containing the same issuer DN and subject DN as the certificate they used to authenticate to the revocation page. Once the revocation request has been submitted, it will be approved automatically. For details, see section *4.6.6 Using Self-service Revocation*.

NOTE: OCSP, RAMI, and self-service revocation settings have already been configured in section *5.1 Prerequisite*.

5.5.5 FDP_STG_EXT.1 Public Key Protection

The TSF implements and also interfaces with the Operational Environment's Operating System to provide access-controlled storage for the trusted certificates and ACLs used to validate login to the TOE's web interfaces via the trusted channel.

The trust anchor list and various ACLs are maintained in the environmental database in tables that can be managed via the Admin Site and command line program (CACLI).

To manage the trust anchor list via the Admin Site, see section *4.4.2.2.1 Certificate and Path Validations.*

To manage the trust anchor list using the CACLI, see section *4.9 Using CertAgent Command Line Tool (CACLI)* and use the following commands:

```
Syntax:

* Display trust anchors
  -showtrust

* Add a trust anchor
  -addtrust -file <cert file>

* Remove a trust anchor
  -removetrust
```

Example:

```
#> ./cacli.sh -showtrust
#> ./cacli.sh -addtrust -file /usr/trust.der
#> ./cacli.sh -removetrust
```

The remove a trust anchor command will be presented with a list of trust anchors and then be prompted to enter the ID of the certificate that you wish to remove from the list or a '*' to remove all the certificates.

To manage the ACLs of Admin Site, CA accounts and profiles, see sections *4.4.7 Managing the Server Administration Access Control List*, *4.4.6.1 Managing the ACL* and *4.5.7.3 Managing Certificate Profiles* respectively.

To manage the ACLs using the CACLI, see section *4.9 Using CertAgent Command Line Tool (CACLI)* and use the following commands:

```
Syntax:

* Display the ACL for a CA account, profile, or Admin Site
  -showacl (-ca <ca name> | -profile <profile name> | -admin) [-acl
<permissions>]

* Add a certificate to the ACL for a CA account, profile, or Admin Site
  -addacl (-ca <ca name> | -profile <profile name> | -admin) -acl <permission>
  -cert <cert file>

* Update the permissions of the ACL for a CA account, profile, or Admin Site
(lists certs and prompts for id to update)
  -updateacl (-ca <ca name> | -profile <profile name> | -admin)

* Remove a certificate from the ACL for a CA account, profile, or Admin Site
(lists certs and prompts for id to remove)
  -removeacl (-ca <ca name> | -profile <profile name> | -admin)

-acl <permissions>     ACL permissions
   an XOR'ed combination of the following values:
       1     admin
       2     audit
       4     certify
       8     revoke
      16     RAMI
      32     DBAccess
```

Example (managing Admin ACL):

```
#> ./cacli.sh –showacl -admin
#> ./cacli.sh –addacl –admin –acl 1 -cert /usr/admin.der
#> ./cacli.sh –updateacl –admin
#> ./cacli.sh –removeacl -admin
```

Example (managing CA Account ACL):

```
#> ./cacli.sh –showacl –ca testca
#> ./cacli.sh –addacl –ca testca –acl 2 -cert /usr/auditor.der
#> ./cacli.sh –updateacl –ca testca
#> ./cacli.sh –removeacl –ca testca
```

Example (managing Admin ACL):

```
#> ./cacli.sh –showacl –profile testprofile
#> ./cacli.sh –addacl –profile testprofile –acl 4 -cert /usr/ca-op-staff.der
#> ./cacli.sh –updateacl –profile testprofile
#> ./cacli.sh –removeacl –profile testprofile
```

NOTE: The '-updateacl' and '-removeacl' commands will be presented with a list of all certificates in the appropriate ACL and then be prompted to enter the IDs of those certificates that you wish to update or remove from the list.

5.5.6 FDP_CRL_EXT.1 Certificate Revocation List Validation

Administrators can configure the CA Account to limit the number of issued CRLs retained, to use a particular message digest algorithm (SHA-384 or SHA-512), validity period, and extensions when issuing a CRL.

CA Operations Staffs with 'revoke' permission can configure CRLs to be automatically issued.

For details on configuring the above settings, see section *4.5.7.5 Managing CRL Issuance.*

5.5.7 FDP_OCSPG_EXT.1 OCSP Basic Response Generation

The TOE produces OCSP basic responses as described in IETF RFC 6960. The OCSP responses are signed by either the CA's issuer private key which resides in the PKCS#11 Cryptographic Module or a delegated OCSP signer credential whose certificate includes the OCSP Signing extended key usage OID and whose private key resides in the PKCS#11 Cryptographic Module. SHA-1, SHA-256, SHA-384, and SHA-512 are supported and can be configured via either the TOE's CA Account web interface (for issuers the TOE is hosting) or by the TOE's Admin Account web interface (for external issuers) by an administrator. OCSP responses are based on CRLs stored by the CA which can be those generated by issuers hosted by the CA itself, or CRLs obtained from external issuers manually or via HTTP.

The following values included in the OCSP response:

- The version fields always contain a 0.

  The signatureAlgorithm field contains the object identifier (OID) for a digital signature algorithm in accordance with FCS_COP.1(2). Depending on the OCSP signer's key type (RSA or ECC) and the hash algorithm selected in the OCSP configuration setting, these OIDs are supported: ecdsa-with-SHA1 (1.2.840.10045.4.1), ecdsa-with-SHA256 (1.2.840.10045.4.3.2), ecdsa-with-SHA384 (1.2.840.10045.4.3.3), ecdsa-with-SHA512 (1.2.840.10045.4.3.4), sha1WithRSAEncryption (1.2.840.113549.1.1.5), sha256WithRSAEncryption (1.2.840.113549.1.1.11), sha384WithRSAEncryption (1.2.840.113549.1.1.12), sha512WithRSAEncryption (1.2.840.113549.1.1.13)
- The thisUpdate field always sets to the time at which the OCSP responder signed the response and the status being indicated is known to be correct. This field is not configurable.
- The producedAt field always sets to the time at which the OCSP responder signed the response. This field is not configurable.

- The time specified in the nextUpdate field does not precede the time specified in the thisUpdate field. This field can be configured to use the same nextUpdate field as in the current CRL or a specific period of time from the thisUpdate field by an administrator.

For issuers the TOE is hosting, administrators can enable or disable OCSP for an issuer by checking or unchecking the 'Enable OCSP Responder' checkbox for the CA account in the OCSP Responder page. Administrators may select the hash algorithm, credential, nonce handling, response caching, and time to live that are used when signing the responses. For details, see section *4.5.7.6 Managing OCSP Responder Settings.*

For external issuers, administrators can enable or disable OCSP for an issuer by adding or removing an account for an external issuer in the Dhuma page of the Admin web interface. Administrators may select the CRL retrieval method, hash algorithm, issuer certificate, OCSP signer credential, nonce handling, response caching, and time to live that are used when signing the responses. For details, see section *4.4.10 Managing Dhuma Accounts.*

5.5.8 FDP_RIP.1 Subset Residual Information Protection

No configurable actions.

5.6 Identification and Authentication (FIA)

5.6.1 FIA_X509_EXT.1 Certificate Validation, FIA_X509_EXT.2 Certificate-Based Authentication

The TOE uses X.509v3 certificates, as defined by RFC 5280, to authenticate privileged users, subscribers, RAs, and DBAccess clients over HTTPS, and to verify the integrity of software updates.

The TOE does not rely on the Operational Environment to perform certificate handling functionality. When the TOE cannot determine the validity of a certificate, the TOE will not accept the certificate. There is no option in the TOE to change this behavior.

To configure the trust anchor list and CRLs for path validation, see section *4.4.2.2.1 Certificate and Path Validations*.

5.6.2 FIA_UIA_EXT.1 User Identification and Authentication

Privileged users, RAMI, DBAccess, EST, and self-service revocation settings have already been configured in section *5.1 Prerequisite.*

By default, all services for privileged user and subscriber self-services require successfully logging in. Other services do not require identification and authentication. There is no option in the TOE to change this behavior.

5.6.2.1 Privileged Users

The TOE uses HTTPS/TLS with certificate-based client authentication as the only method for privileged users to login to the Admin, CA Account Sites, RAMI, DBAccess, and EST. The client certificate must pass the TOE's certificate path validation with CRL checking

To login to the Admin Site, follow the steps in *4.4.1 Logging in the Administrative Site*. Once the privileged user logged in successfully, a status page showing "You are currently logged in as the site <administrator or auditor> (<subject DN of the certificate>)." will be displayed. Otherwise, an error page with "You are not an authorized user: <subject DN of the certificate>" will be displayed.

To login to the CA Site, follow the steps in *4.5.1 Logging in the CA Account Site*. Once the privileged user logged in successfully, a status page showing "You are currently logged in as an authorized user (<subject DN of the certificate>) with <permission> rights." will be displayed. Otherwise, an error page with "You are not an authorized user: <subject DN of the certificate>" will be displayed.

To submit requests via the RAMI or DBAccess, follow the steps in section *4.7 Using RAMI* and *4.8 Using Database Access Service*. If the user is authorized ("successful logon"), the specified request will be processed, and the result will be returned. Otherwise, an error message "You are not an authorized user" will be returned in the response.

The TOE's EST implementation supports client authorization defined in section 3.7 of RFC 7030 that states that the client is a Registration Authority if the client authentication certificate used was issued by the EST CA, and it includes the id-kp-cmcRA OID in its extendedKeyUsage extension. In this case the EST client is treated as an RA, not a subscriber. To submit EST enrollment requests as an RA, follow the steps in section *4.5.7.1.3 EST (Enrollment over Secure Transport).* If the RA is authorized ("successful logon"), the issued certificate and its chain will be returned in the response. Otherwise, HTTP response code 400 (bad request) will be returned along with the detailed error message in the response.

To execute the TOE's command line tools requires an authorized user to login in to the environmental Operating System with administrator rights. If the user is authorized, the request command will be processed. Otherwise, an "Access is denied" message will appear in the result.

5.6.2.2 Subscribers

Subscribers may submit certificate requests using either the TOE's Public site or through EST. Using the TOE's Public site, a subscriber may, without identification and authentication, submit a certificate request. Certificate requests received in this manner are manually verified by having the subscriber confirm the request ID displayed post submission to a privileged user using an out-of-band communication method prior to issuance.

The TOE supports two subscriber self-service requests: revocation and certificate enrollment via EST. These self-services have already been configured in section *5.1 Prerequisite*.

The self-service revocation requires subscribers to successfully authenticate to the TOE using TLS/HTTPS with client authentication using their valid certificate issued in a manner matching that of privileged users. Once the subscriber has been authenticated ("successful logon"), only certificates matching the Subject DN in the certificate used to authenticate are presented to the subscriber for self-revocation. Otherwise, a page will be displayed with an error message (e.g., "You are not authorized to manage your certificate (<subject DN of the certificate>) from this CA account").

The EST service requires subscribers to successfully authenticate using an EST subscriber name and password or their valid certificate. If a subscriber is authenticated, the issued certificate and its chain will be returned in the response. Otherwise, the HTTP response code 400 (bad request) will be returned along with the response's detailed error message.

5.6.2.3 Relying Parties

Relying parties are never authenticated or identified. Relying parties may use the TOE's Public site to obtain certificate status information by downloading CRLs, or certificates, by downloading root certificates, issuer certificates, or subscriber certificates. Relying parties may also use the OCSP interface to obtain certificate status information.

5.6.3 FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server

EST setting has already been configured in section *5.1 Prerequisite.*

5.6.4 FIA_X509_EXT.3 X509 Certificate Request

The TOE supports the generation of a PKCS#10 certificate request when establishing a subordinate CA or when cross-certification with another issuer is desired.

To generate a certificate request and configure the CA distinguish name for a subordinate CA, follow the steps in section *4.5.3.2 Generating Credential for Subordinate CA.*

To generate a certificate request for cross-certification, follow the steps in section *4.5.3.3 Exporting Credentials.*

5.6.5 FIA_ENR_EXT.1.1 Certificate Enrollment

An external certification authority can be used to issue the CA's certificate managed by the TOE. To generate a certificate request to an external certification authority, see the steps in section *4.5.3.2.1 External CA*.

5.7 Security Management (FMT)

5.7.1 FMT_MOF.1 Management of Security Functions Behavior

The role restriction mechanism is not configurable. For details on role restriction, see section *4.4.2.2.2 Restrictions on Security Roles*.

5.7.2 FMT_MTD.1 Management of TSF Data

The administrative functions listed below are accessible through the TOE's web interfaces. For details on role restriction, see section *4.4.2.2.2 Restrictions on Security Roles*. Only privileged users with appropriate roles and permissions can access their functions.

The Operational Environment restricts the following tasks to the local administrator. The local administrator is required to have login access to the operational environment with read, write, and execute permissions to the TOE's installation directory.

1. manage the TOE locally;
2. perform updates to the TOE;
3. perform destruction of sensitive data when no longer needed;
4. participate as a second party for archival and recovery;
5. perform encrypted export of private or secret key or critical data

The TOE restricts the following tasks, performed through the TOE web interface Admin Site, to the Administrator role:

1. manage the TOE locally and remotely;
2. manage the audit mechanism;
3. perform on-demand integrity tests;
4. import and remove X.509v3 certificates into/from the Trust Anchor Database;
5. manage the ACL of the Admin Site and CA Site;
6. manage the CRL store for path validation;
7. configure the default TOE access banner;
8. disable CA accounts;
9. configure OCSP function;

The TOE restricts the following tasks, performed through the TOE web interface CA Account Site, to Administrator role:

1. configure and manage certificate profiles;
2. modify revocation configuration;
3. configure certificate revocation list function;

4. configure OCSP function;
5. export PKCS#10 certificate request;
6. import CA certificate;
7. generate certificate request for issuer;

The TOE restricts the following tasks to CA Operations Staff with 'certify' permission of the given CA Account Site:

1. approve and execute the issuance of certificates;
2. configure subscriber self-service request constraints (EST users);
3. configure automated certificate approval management;

The TOE restricts the following tasks to CA Operations Staff with 'revoke' permission of the given CA Account Site:

1. approve certificate revocation; including the ability to configure automatic CRL issuance
2. configure subscriber self-service request constraints (revocation service);

The TOE restricts the following tasks to Auditors with access to the given site:

1. Search the audit trail

5.7.3 FMT_SMF.1 Specification of Management Functions

The TSF performs the following management functions. Details on each functions are also listed.

1. Ability to manage the TOE locally and remotely;
   - Section 4.1 Starting and Stopping the Service
   - Section 4.4 Managing the Administrative Site
   - Section 4.5 Managing the CA Account Site
   - Section 4.7 Using RAMI
   - Section 4.8 Using Database Access Service
   - Section 4.9 Using CertAgent Command Line Tool (CACLI)
2. Ability to perform updates to the TOE;
   - Section 4.10 Updating the TOEUpdating
3. Ability to perform archival and recovery;
   - Thales Luna USB HSM documentation
4. Ability to manage the audit mechanism;
   - Section 4.4.4 Configuring Audit Trail Settings

5. Ability to configure and manage certificate profiles;
    - Section 4.5.7.3 Managing Certificate Profiles
    - Section 4.5.7.4 Managing Certificate Issuance
6. Ability to approve and execute the issuance of certificates;
    - Section 4.5.4.3 Issuing Certificates
7. Ability to approve certificate revocation;
    - Section 4.5.5.3 Revoking Certificates
8. Ability to modify revocation configuration;
    - Section 4.5.7.8 Managing Revocation Policy
    - Section 4.5.7.5 Managing CRL Issuance
    - Section 4.5.7.6 Managing OCSP Responder Settings
9. Ability to configure subscriber self-service request constraints;
    - Section 4.5.7.9 Managing Self-Service Settings
10. Ability to perform on-demand integrity tests;
    - Section 4.4.2.1.2 Running Integrity Test on Demand
11. Ability to destroy sensitive user data when no longer needed;
    - Thales Luna USB HSM documentation

    NOTE: No sensitive user data is maintained by the TOE
12. Ability to import and remove X.509v3 certificates into/from the Trust Anchor Database;
    - Section 4.4.2.2.1 Certificate and Path Validations
13. Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate;
    - Section 4.5.7.5 Managing CRL Issuance
14. Ability to modify the CRL configuration
    - Section 4.5.7.5 Managing CRL Issuance
    - Section 4.5.7.8 Managing Revocation Policy
15. Ability to modify the OCSP configuration
    - Section 4.4.10.2.4 Configuring OCSP Response Settings
    - Section 4.5.7.6 Managing OCSP Responder Settings
16. Ability to configure the cryptographic functionality;
    - The asymmetric algorithm used for the System credential
        - Section 4.4.8 Managing System Credential
    - The asymmetric algorithm used for an Issuer or Root credential
        - Section 4.5.3 Managing CA Credentials
    - The message digest used when issuing CRLs

- Section 4.5.7.5 Managing CRL Issuance (message digest used when issuing CRL)

- The message digest used when creating OCSP responses
  - Section 4.4.10.2.4 Configuring OCSP Response Settings
  - Section 4.5.7.6 Managing OCSP Responder Settings
- The message digest used when issuing certificates
  - Section 4.5.7.4 Managing Certificate Issuance
- The asymmetric algorithms that the TOE will accept in certificate requests
  - Section 4.5.7.1 Managing Certificate Enrollment
- The cryptographic functionality for the PKCS#11 Cryptographic Module
  - Thales Luna USB HSM documentation
- The TLS version 1.2 and ciphersuites used in TLS/HTTPS
  - The supported ciphersuites (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) can be configured by a local Administrator using the environmental Operating System's text editor to modify the TOE's configuration file (<ca home>/tomcat/conf/server.xml)
  - The TLS version 1.2 is not configurable

5.7.4 FMT_SMR.2 Restrictions on Security Roles

Sections 1.5 Privileged User Roles and *1.4 Interfaces* describe the roles and interfaces supported by the TOE and how the roles connect to these interfaces and perform operations.

To assign Administrator or Auditor Role to users on the Operational Environment, see section *2.1.1 Creating Privileged Users*.

To assign roles to users to access Admin site:

1. Follow the steps in section *4.4.7 Managing the Server Administration Access Control List* .
2. To add an administrator, upload the administrator certificate and select 'admin' permission.
3. To add an auditor, upload the auditor certificate and select 'audit' permission.

To assign roles to users to access CA Account site, RAMI, and DBAccess:

1. Follow the steps in section *4.4.6.1 Managing the ACL.*
2. To add an administrator, upload the administrator certificate and select 'admin' permission.

3. To add an auditor, upload the auditor certificate and select ‘audit’ permission.
4. To add a CA operations staff, upload the CA operations staff certificate and select ‘certify’, ‘revoke’, ‘RAMI’, and/or ‘DBAccess’ permissions.

5.8 Protection of the TSF (FPT)

5.8.1 FPT_FLS.1 Failure with Preservation of Secure State

The TOE preserves a secure state when the following types of failures occur: RBG failure, ISC CDK failure, integrity failure on Trust Anchor list or ACLs, PKCS#11 Cryptographic Module failure, and database failure.

When the TOE detects a failure in itself that prevents operations from continuing, it shuts itself down in an orderly manner. This shutdown process is the same process that is used to shut down the TOE prior to a system restart. Plaintext keys and unencrypted user data are cleared from memory during this process leaving only encrypted keys and encrypted user data within the environmental storage.

Once the TOE has been shut down, no services will be available. A local administrator must login to the Operational Environment and identify the error from the local server log file.

The TOE detects failures in the Operational Environment by checking the status indicator of the PKCS#11 Cryptographic module (API function return codes) and by catching exceptions thrown by the JDBC API used to communicate with the database. When the TOE detects a failure in the Operational Environment that can be corrected while the TOE is still running, it creates audit records and returns an error message. If the TOE detects a failure in the Operational Environment that cannot be corrected while running, it shuts itself shown in an orderly fashion as described above.

Below sections describe the actions that might occur and provides remedial instruction for each type of failure.

5.8.1.1 ISC CDK/RGB Failure

ISC CDK failure causing the hard error state, including a failure of the DRBG. On failure, the TOE aborts the action, returns the error message to the caller, records the error in the audit trail, and local server log file, destroys any sensitive data, and shuts down the TOE service.

A local administrator must restart the TOE. For details, see section *4.1.1 Managing the TOE Service.*

5.8.1.2 Integrity Failure on Trust Anchor List or ACLs

On integrity failure on trust anchor list or ACLs, the TOE returns the error message to the caller, records the error in the audit trail and local server log file, destroys any sensitive data, and shuts down the TOE service.

A local administrator must restart TOE in maintenance mode which will disable the data integrity on trust anchor list and ACLs, integrity test, path validation, and security role restriction. Only the Admin Site will be accessible by privileged users. For details, see section *4.1.2 Starting the Service in Maintenance Mode*.

An administrator of the Admin Site then needs to remove all certificates from the corresponded list and reimport the certificates to the list via the web interface or CACLI.

To manage the trust anchor list via the Admin Site, see section *4.4.2.2.1 Certificate and Path Validations.*

To manage the ACLs of Admin Site, CA accounts, and profiles, see sections *4.4.7 Managing the Server Administration Access Control List*, *4.4.6.1 Managing the ACL* and *4.5.7.3 Managing Certificate Profiles* respectively.

To manage the trust anchor list and ACLs via the CACLI, see section *4.9 Using CertAgent Command Line Tool (CACLI).*

Once the trust anchor list or ACLs have been recreated, follow the steps in section *4.4.2 Managing NIAP Conformance Settings* to enable the data integrity, path validation, and security role restriction settings which have been disabled in maintenance mode. Enabling the NIAP options causes the signatures over the trust list and ACLs to be computed and stored restoring the integrity of the system.

A local administrator must then restart the TOE (in non-maintenance mode) to resume the regular operations of the TOE. For details, see section *4.1.1 Managing the TOE Service.*

5.8.1.3 Database Inaccessible

On database inaccessible failure, the TOE aborts the action, returns the error message to the caller, records the error in the local server log file, destroys any sensitive data, and shuts down the TOE.

A local administrator must correct the database issue (examine the database logs, correct the issue, and restart the database), and then restart the TOE. For details, see section *4.1.1 Managing the TOE Service.*

5.8.1.4 PKCS#11 Failure

On PKCS#11 failure, including failure of the device's DRBB, the TOE aborts the action, records the error in the audit trail, and returns the error message to the caller. The TOE does not shut down in this case.

A local administrator must correct the PKCS#11 issue (examine the PKCS#11 library, connectivity, keys on the device, etc.). Restart the TOE may be required if the PKCS#11 fixes do not take effect immediately. For details on start the TOE, see section *4.1.1 Managing the TOE Service.*

5.8.2 FPT_KST_EXT.1 No Plaintext Key Export, FPT_KST_EXT.2 TSF Key Protection

Neither the TOE nor the PKCS#11 Cryptographic Module in the OE provides a mechanism for plaintext key export.

By default, the TOE restricts access to operations that would use the issuer keys using client authenticated web pages. No user can use any key unless they've been successfully authenticated as a privileged user. Thus the TOE ensures that unauthorized users and unprivileged processes cannot access its private and secret keys.

The HSM provides its own protection mechanisms to prevent unauthorized users and unprivileged processes access to its protected functions and data. The TOE must authenticate to the PKCS#11 Cryptographic Module when the TOE starts using a password in order to access the cryptographic services of the PKCS#11 Cryptographic Module.

There is no configuration on the TOE or the PKCS#11 Cryptographic Module to change the above behavior.

5.8.3 FPT_RCV.1 Manual Trusted Recovery

After a failure of integrity is detected, the TOE shuts itself down in an orderly manner. To return the TOE to a secure state, a local administrator must restart TOE in maintenance mode. For details, see section *4.1.2 Starting the Service in Maintenance Mode*.

NOTE: For other types of failure (ISC CDK, RGB, database, or PKCS#11), the TOE does not have to operate in maintenance mode in order for the TOE to return to a secure state.

When the TOE is in maintenance mode, the TOE prevents normal operations and limits privileged user, subscriber, and relying party actions so that only an administrator may log on and correct the integrity failure. All other functions (EST, OCSP, issuance, etc.) are disabled. When in maintenance mode, the NIAP restrictions that are not enforced are:

- Requiring data integrity on the Trust Anchor list used for certificate path validation
- Requiring data integrity on the ACLs
- Checking integrity of the Trust Anchor and ACLs when the TOE starts
- Using strict certificate path validation
- Enforcing role separation

To restore a secure state in the case of integrity failure, an administrator needs to remove all certificates from the corresponded list and reimport the certificates to the list via the Admit Site or CACLI.

To manage the trust anchor list via the Admin Site, see section *4.4.2.2.1 Certificate and Path Validations.*

To manage the ACLs of Admin Site, CA accounts, and profiles, see sections *4.4.7 Managing the Server Administration Access Control List*, *4.4.6.1 Managing the ACL* and *4.5.7.3 Managing Certificate Profiles* respectively.

To manage the trust anchor list and ACLs via the CACLI, see section *4.9 Using CertAgent Command Line Tool (CACLI).*

Once the trust anchor list or ACLs have been recreated, follow the steps in section *4.4.2 Managing NIAP Conformance Settings* to enable the data integrity, path validation, and security role restriction settings which have been disabled in maintenance mode. Enabling the NIAP options causes the signatures over the trust list and ACLs to be computed and stored restoring the integrity of the system.

A local administrator must then restart the TOE (in non-maintenance mode) to resume the regular operations of the TOE. For details, see section *4.1.1 Managing the TOE Service*.

5.8.4 FPT_SKP_EXT.1 Protection of Keys

The TSF provides no mechanisms allowing the reading of any pre-shared, private, or secret keys. The PKCS#11 Cryptographic Module maintains its own protections of keys it holds, and in the evaluated configuration does not provide any mechanism for reading those keys.

5.8.5 FPT_STM.1 Reliable Time Stamps

Timestamps are based on the environmental Operating System's clock and managed by the environmental Operating System. The TOE does not support the use of a network time protocol (NTP) server.

To change the time and date on CentOS:

1. Login to the CentOS as OE administrator.
2. Open a Terminal and enter the following commands:

```
sudo date <date in MMDDhhmmYYYY.ss format>
sudo hwclock --systohc
```

   For example, for September 02, 2020 1:00:00pm, enter `090213002020.00` for the `date` command.

To change the time and date on Windows 2016:

1. Login as administrator, right-click the current time in the system tray and select **Adjust date/time** from the context menu.
2. Click **Change date and time**. Make the changes as desired and click **OK**.
3. To change the time zone, click **Change time zone.** Make the changes as desired and click **OK**.

5.8.6 FPT_TUD_EXT.1 Trusted Update

For details on verifying the TOE version and updating the TOE, see section *4.10 Updating the TOE*.

5.8.7 FPT_TST_EXT.2 Integrity Test

The TOE supports data integrity on the trust anchor list and ACLs. The TOE verifies the integrity of the Trust Anchor and ACL tables when the TOE starts, whenever any protected table is changed, and on-demand when requested through the NIAP section of the Admin Site. On integrity failure, the TOE returns the error message to the caller, records the error in the audit trail and local server log file, destroys any sensitive data, and shuts down the TOE service.

When the TOE starts, the TOE verifies the integrity of the trust anchor list and ACLs automatically and records the result to the audit trail. Below are the sample events:

```
Started integrity test on startup
Ran integrity test on the Trust Anchor database: passed
Ran integrity test on the ACL database: passed
Completed integrity test on startup
```

To verify the integrity manually, follow the steps in section *4.4.2.1.2 Running Integrity Test on Demand.*

5.9 TOE Access (FTA)

5.9.1 FTA_SSL.4 User-initiated Termination

Privileged users logged in to the Admin or CA Account Site can click the **Log Out** button from the left panel to terminate the current session.

5.9.2 FTA_TAB.1 Default TOE Access Banners

To manage the access banner, see section *4.4.2.8 Access Banner*.

5.9.3 FTA_SSL.3 TSF-initiated Termination

The TOE supports an administratively defined TLS/HTTPS session timeout. The default session time-out value for administrative and CA account logins is 30 minutes.

To change the TOE's session time-out:

1. Append the following option to the CATALINA_OPTS variable to the Tomcat's startup script (`<ca home>/tomcat.sh` or `<ca home>\tomcat.bat`):

   ```
   -Disc.ca.web.session.timeout=<time-out value in minutes>
   ```

   NOTE: Minimum and maximum session time-outs are 1 and 35791394 minutes respectively. An integer that is out of this range indicates the session should never time-out and shouldn't be specified.

2. Restart the TOE. For details, see section *4.1.1 Managing the TOE Service.*

5.10 Trusted Path/Channels (FTP)

5.10.1 FTP_TRP.1 Trusted Path

The TSF also uses client authenticated HTTPS to provide a trusted communication path between itself and remote subscribers and privileged users.

The following interfaces require privileged users to establish a trusted path/channel using TLS with client authentication.

Remote Interface	Details
Admin site	Section 4.4.1 Logging in the Administrative Site
CA site	Section 4.5.1 Logging in the CA Account Site
DBAccess API	Section 4.8 Using Database Access Service
RAMI API	Section 4.7 Using RAMI

The following interfaces require subscribers to establish a trusted path/channel using TLS with client authentication.

Remote Interface	Details
Public site (self-service)	Section 4.6.6 Using Self-service Revocation
EST (client authentication)	Section 4.5.7.1.3 EST (Enrollment over Secure Transport)

The following interfaces require subscribers to establish a trusted path/channel using TLS without client authentication.

Remote Interface	Details
Public site (certificate enrollment)	Section 4.6.3 Browser-based Certificate Enrollment Section 4.6.4 Uploading a Certificate Request
EST (basic authentication)	Section 4.5.7.1.3 EST (Enrollment over Secure Transport)

All the above interfaces must be connected via HTTPS/TLS. If non-TLS port is specified in the access URL, requests will be rejected.

5.10.2 FTP_ITC.1 Inter-TSF trusted channel

The following IT entities are supported.

IT Entity	Protocol	Comments
Audit server	HTTPS	Client authenticated using the DBAccess API
RA	HTTPS	Client authenticated using the RAMI API

To establish a connection to the audit server, follow the steps in Section 4.8 Using Database Access Service. In the client program, specify the privileged user with auditor role and use the `queryAdminAuditTrail` and `queryCAAuditTrail` methods in the API to retrieve the audit trail records of the Admin site and CA account respectively.

To establish a connection to the RAMI, follow the steps in section *4.7 Using RAMI*.

NOTE: A new HTTPS connection is established for each request submitted to the DBAccess and RAMI API. If the HTTPS connection is interrupted, it cannot be recovered. Simply resubmit the request.