HP OpenView Select Federation

For the HP-UX, Linux, Solaris and Windows® Operating Systems

Software Version: 6.60

Certificate Management User's Guide

Document Release Date: November 2006
Software Release Date: November 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

HP OpenView Select Federation includes software developed by third parties. The software in Select Federation includes:

- Apache Derby, Apache Xalan Library, Apache Xerces Library, and Apache XML Dsig Library.
- Software developed by the University Corporation for Advanced Internet Development <http://www.ucaid.edu>Internet2 Project.

Trademark Notices

- Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
- Microsoft®, Windows®, and Windows XP® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- UNIX® is a registered trademark of The OpenGroup.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

Certificate Management Tool (CMT) is a platform independent software tool implemented in Java which can be used to manage keystores and its individual key and certificate entries. This tool exclusively uses Java Cryptography Architecture and supports the JKS file format. This tool does not require any console-based operation.

CMT supports the following operations:

- Create new keystores
- Modify current keystores
  - Creating self-signed certificates in `X.509` format
  - Creating `PKCS#10` certificate signing request (CSR)
  - Deleting existing entries
- Import to current keystore
  - Existing third-party signed certificates
  - Self-signed certificates
  - `PKCS#12` file containing key and certificate
- Export from current keystore
  - Key in `X.509` format
  - Certificate in `X.509` format
  - Key and certificate to `PKCS#12` file
  - CSR request to `PKCS#10` file
- Display current keystore entry details
  - **List view**: all entries are displayed in a tree structure
  - **Detailed view**: entry details are displayed in tabular format
  - **PEM view**: `PEM`-encoded display of the selected entry

The Certificate Management Tool (CMT) is a standalone 100% Pure Java application. When you run the Select Federation Installer, the CMT is installed in the `tools/cmt` directory.

Running the CMT

To launch the CMT, execute the following command appropriate for your operating system:

- On Linux:

  `./cmt.sh`

- On Windows:

```
C:\Program Files\HP OpenView\Select Federation\tools\cmt> cmt.bat
```

Before running the tool, be sure that all the configuration parameters are set according to the requirements. See all the configuration parameters in the next section Configuring the CMT.

Configuring the CMT

CMT can be configured by modifying the configuration properties in the `config.properties` file. Details of the configuration properties are in the following sections:

- Logging-Related Properties
- Tool-Related Properties

Logging-Related Properties

handler

This property is a logging handler, which logs logging messages. There are two types of logging handlers:

- `java.util.logging.FileHandler` – This handler is the default, which logs messages to a specified file on the disk.
- `java.util.logging.ConsoleHandler` – This handler prints messages directly on the console.

java.util.logging.ConsoleHandler.level

This property specifies the logging level for the console handler. The default is set to OFF so that no logging messages are displayed on the console.

java.util.logging.FileHandler.level:

This property specifies the logging level for the file log handler. The default is set to SEVERE. Other possible values are WARNING, INFO, ALL, FINE, FINER, FINEST (in descending order of debug information). The value should be kept low if you need the debug messages. Otherwise, keep the values high (SEVERE).

java.util.logging.FileHandler.pattern

This property specifies the file in which log messages are to be stored. The default file name is `cmt.log`.

java.util.logging.FileHandler.formatter

This property specifies the format in which logging messages are to be printed in the file. There are two types of logging formatters:

- `java.util.logging.SimpleFormatter` — This logging format is the default, which formats the logs in plain text readable format.

- `java.util.logging.XMLFormatter` — This logging format formats the logs in xml format. Each message is entered as a new element and each informational unit is entered as a separate node in that element.

Tool-Related Properties

JCEProvider

This property specifies which JCE provider to use. There are two types of JCE providers supported by this tool.

- BC (Bouncy Castle) — BC is the default value for the JCE provider. The BC provider is widely used and supports a large number of encryption algorithms and a wide range of key sizes. See **http://www.bouncycastle.org** for more information. This provider is bundled with the CMT.
- SUN (Sun JCE provider) – The SUN JCE provider is used by default with Java JDK or JRE.

historyfile

This property provides a keystore history in a flat file called `history.properties in` the `install` directory. This file maintains the history of the last five keystores that were used.

2 Supported Features

The Certificate Management Tool (CMT) supports various keystore management operations. You can invoke these operations through selecting the menus or clicking on the tools on the toolbar. This chapter describes the menus and the menu options.

The CMT manages one “keystore” at a time. A keystore is a single file in JKS format, which can contain keys, certificate signing requests (CSRs) and certificates. Using the CMT, you can generate new keypairs, import or export certificates or generate CSRs.

File Menu

Create New Keystore

You can create a new keystore using CMT. CMT asks the user to enter the location and password for the keystore file. On submitting this information, an empty keystore is created at the given location and is protected by the given key-password. You need to save the newly created keystore to use it afterwards.

Open Keystore

Opening the keystore makes it available for other operations. Once opened, all the contents of the keystore are visible in the tree structure under **List View**. If an individual entry in the **List View** is selected, the detailed view of the selected entry displays in the right pane. The detailed view can be shown in `PEM` or tabular format. Select the format you want in the **View** menu.

Load Recent Keystore

CMT stores the history of five recently opened keystores. You can select one of them by using this feature. In this case, the key-password of the selected keystore is required to open the keystore. You do not need to browse for the file in the file system.

Save Keystore

Any modifications done in the keystore are written to the current keystore using the **Save Keystore** sub-menu.

Close Keystore

To operate another keystore without restarting the CMT, close the current keystore and open another one. If any unsaved modifications have been done in the current keystore, the CMT prompts you to save the keystore.

Edit Menu

Create New Entry

To create a new entry, enter the following information:

- **Alias*** **(**name of the entry in the keystore)
- **Password*** (password for the key/certificate entry)
- **Name of creator***
- **Name of organization***
- **Email Id**
- **Organization unit**
- **Town**
- **State**
- **Country**
- **Keysize*** (512,1024,2048) in bits
- **Validity period*** (days/weeks/months/years)

The fields identified with an * are required. These field values are included in the CSR or certificate that is generated along with the key pair.

You can create two types of new entries in the keystore.

- Certificate Signing Request(CSR):

  All information entered when creating the entry is used in the Certificate Signing Request (CSR). The CSR is created in `PKCS#10` format. This operation creates a CSR entry in the keystore. It also allows you to save the CSR into a file. Since keystores cannot have entries without certificates, the CMT generates a dummy certificate with serial number -1. This way, the CSR can be sent to the CA for certificate signing and the signed certificate could be imported.

- Self Signed Certificate (SSC):

  Self-signed certificates may be used where a third-party trust is not required by the application. Users can generate self-signed certificates using this feature. For a self-signed certificate, the key pair and self signed certificate in `X.509` format is created from the user entered information. A new entry is added to the keystore.

Delete Entry

Any available entry (key, certificate, CSR) in the keystore can be deleted. Only one entry can be deleted at a time. Before any delete, the CMT asks for user confirmation of the particular delete operation.

View Menu

Show Details in Table Format

Contents of the selected entry are shown in tabular format as Attribute and Value. Following are the contents of the table format:

- Serial Number
- Version
- Issuer DN
- Subject DN
- Valid (If certificate is not valid, this field will show “NO” in red color.)
- Valid From
- Valid Till
- Signature Algorithm
- Public Keysize
- MD5 Fingerprint
- SHA-1 Fingerprint

Show Details in PEM Format

Contents of the selected entry are shown in `PEM` encoded format. You can select the required part and copy and paste it to wherever you wish.

Import Menu

Import Certificate

Import an existing third-party or self-signed certificate in the keystore.

If the private-key corresponding to the certificate being imported already exists, the certificate is added to the alias corresponding to that key. Otherwise, a new certificate entry is created in the keystore.

A third-party certificate is one in which the corresponding private-key is not in the keystore. If the certificate being imported is a third-party certificate, the tool asks whether to add the certificate as a “Trusted Certificate.”

To import a third-party or self-signed certificate, you need to specify the following:

- **Alias** to which the certificate will be imported.
- **Key password** for the alias.
- **File** containing the certificate to be imported.

Import Key and Certificate

The CMT has two options for importing keys and certificates. The key and the certificate may be in separate files, or they may be in a single `PKCS#12` format file. To import an existing key and certificate from separate files in the keystore, click **Import** → **Import Key and Certificate**.

If the key and certificate already exists with the same alias name, then the tool asks whether to overwrite the entry. Also, if the key already exists with a different alias name, then the tool asks whether to create a new entry with a new alias name. For that user, you need to specify the following:

- **Alias** to which the certificate will be imported.
- **Key password** for the alias.
- **File** containing the certificate to be imported.
- **File** containing the key to be imported.

Import PKCS#12 Certificate

If the keys and certificates to be imported are in a single `PKCS#12` file, click **Import** → **Import PKCS#12 File**. You need to specify the following:

- **Alias** to which the certificate will be imported.
- **Key password** for the alias.
- **Password** for the PKCS#12 certificate file.
- `PKCS#12` **file path**.

Export Menu

Export Key

Exports the key with the specified alias to a file. The key corresponding to the selected alias is exported to a specified file on disk in `X.509` encoded format. You need to specify the following:

- **Alias** for the key entry in the keystore.
- **Password** for the key entry in the keystore.
- **File** on the disk in which the key will be stored.

Export Certificate

Exports the certificate corresponding to the alias to a file. The certificate corresponding to the selected alias is exported to a specified file on disk in `X.509` format. You need to specify the following:

- **Alias** for the certificate entry in the keystore.
- **Password** for the certificate entry in the keystore.
- **File** on the disk in which certificate will be stored.

Export to PKCS#12 File

Exports either a key and certificate or a third-party certificate to a `PKCS#12` file. A new `PKCS#12` file is created which is protected by the given password. You need to specify the following:

- **Alias** for the entity.
- **Password** for the selected entry.
- **File** on the disk in which key will be stored.
- **Password** for the `PKCS#12` file

Export Certificate Request

Exports a certificate request generated by CMT, which already exists in the keystore. This CSR is exported as a `PKCS10` file and is stored on the disk at a given location. For that user, you need to specify the following:

- **Alias** for the CSR entry.
- **Password** for the specified alias.
- **File** on the disk in which CSR will be stored on export.

For a password (key or cert store) length greater than or equal to 8 characters, you need to download and install “Unlimited Strength” Jurisdiction Policy Files. See **http://java.sun.com/products/jce/index-14.html**.

Glossary

Access Control

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

ADFS (WS-Federation 1.0)

Active Directory Federation Services (ADFS) is a feature of Microsoft Windows 2003 Server R2. ADFS allows a federation with Active Directory-based users, by using the WS-Federation 1.0 protocol.

Administrator

An identity with full permission to manage Select Federation.

Application Helper

Select Federation component that helps you configure URLs in your application for seamless navigation to the Service Provider (SAML Consumer) sites or for authentication through the Identity Provider (SAML Producer) sites.

Application Site Role

An application site (also called a SAML Consumer or Service Provider (SP) Site), which is a Trusted Partner site that participates in a federation to provide a service or application to common users and relies on an authority site to provide authoritative user authentication and other information. For example, in a federation of an extranet with partners' corporate portals, the site hosting the extranet is the application site.

ASP

Microsoft Active Server Pages log users in by invoking the IDP-FSS over a secure channel.

Attribute

One or more characteristics that are part of an identity profile. Attributes are name/value pairs with a type that is assigned a value. For example, an attribute called "Department" may be assigned the values of, "IT", "Sales", or "Support". These attributes are interpreted and assigned appropriately to profiles in different applications (LDAP-compliant directories, databases, SAPs, and so on) based on the mapping rules defined for that application.

Authentication

The act of verifying the credentials of an identity and matching them with an identity profile. The evaluation of credentials ensures that the identity is truly who or what they claim to be.

Authority Site Role

An authority site (also called a SAML Producer or Identity Provider (IDP) Site), which is a Trusted Partner site that participates in a federation to authenticate users and provide other authoritative user information to other sites. For example, in a federation of an extranet with partners' corporate portals, the portals act as the authority site.

Authorization

The process of defining and enforcing the entitlements of an identity. Authentication is a prerequisite for authorization. See Access Control and Authentication.

CA

Certificate Authority

CSR

Certificate Service Request

Delegated Administrator

An identity that has been added by the root administrator. The delegated administrator can perform all functions that the root administrator performs except admin-related functions such as add and remove admins and change admin passwords. When Select Federation is running in Standalone mode, the delegated administrator also cannot view the Admin Audit log. But when Select Federation is integrated with Select Access, then the delegated administrator can view the Admin Audit log. See Root Administrator.

DS

Discover Service

DST

(Data Services Template) DST-based services such as the Personal Profile service (ID-PP) and the Employee Profile service (ID-EP).

Federation

The combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries.

ID-WSF

Liberty Identity Web Services Framework security mechanism.

IDP

An Identity Provider or IDP is an organization or web site that asserts the identity of users to the Service Providers or SPs in a federated network. The assertion of the user identity is done using standard protocols such as SAML and Liberty.

IDP-FSS

IDP filter-support service, which is a servlet component of the Integrated Windows Authentication (IWA). The IDP-FSS enables a trusted program to add a Windows-authenticated user ID into an IDP session.

IIS

The Internet Information Server (IIS) is the web server that is bundled with Windows 2003 Server.

Integrated Windows Authentication (IWA)

Allows Select Federation to leverage a user's Windows logon credentials to seamlessly authenticate the user and transfer the user to a Trusted Federation Partner site.

Keystore

A keystore is a database of keys. The private keys are associated with a certificate chain, which authenticates the corresponding public key. The keystore also contains certificates from trusted entities. By generating the keystore, you add another layer of security to the data that is exchanged in the Select Federation system.

LDAP (Lightweight Directory Access Protocol)

A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network identity can access any resource without knowing where or how it is physically connected.

LECP

Liberty Enabled Client/Proxy Service.

MMC

Microsoft Management Console, used to set up server authentication and to import the `pkcs` / `pfx` format file into your local store on the IIS machine.

NTLM

NT LAN Manager [web definition: is a challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0.]

Protected URLs

Protected URLs require users to be authenticated to allow access to these URLs. If a user is not authenticated, the filter redirects the user to Select Federation for authentication. The Select Federation installation may authenticate the user locally or initiate federated login at another Authority (IDP).

Passive URLs

Passive URLs are for resources where users' personalized content is not critical for the application. Users are allowed to access these URLs even though they cannot be authenticated without being prompted. However, if the user is already logged in at the IDP, has a federation session with Select Federation, or can be authenticated without being prompted, the user's identity and attribute information is presented in the federation session to the application.

Presence Service

A service that informs the WSC if a user is online, available, and so on.

Root Administrator

The “super user” administrator who has complete entitlement to all functionality in the Select Federation Administration Console. The root administrator’s login is always “admin”. Only the root administrator can add and remove delegated administrators and change administrators’ passwords. See Delegated Administrator.

SOAP

Simple Object Access Protocol is a fundamental web services standard for XML-based communication between web service providers and consumers.

SP

A Service Provider (SP) is an application that allows authenticated access based on an authentication performed by an IDP using a federated identity protocol such as Liberty or SAML.

SSL

Secure Sockets Layer handshake protocol, which supports server and client authentication.

SSO

Single Sign-On session/authentication process that permits a user to enter one set of credentials (name and password) to access multiple applications. A Web SSO is a specialized SSO system for web applications.

SAML

Security Assertion Markup Language protocol.

Unprotected URLs

Unprotected URLs allow users access to these URLs without being authenticated. Typically, special URLs such as the login URL and logout URL are unprotected URLs.

WSC

A Web Service Consumer (WSC) is an application that uses web services. It may not be a web service in itself, but uses XML and typically SOAP-based communication with a web service to perform some of its functions.

WSP

A Web Service Provider (WSP) is a web service application that services requests it receives based on XML and typically SOAP-based communication.


invent


Java™
COMPATIBLE