PingFederate®

X.509 Certificate Integration Kit

Version 1.1

User Guide

PingIdentity®

PingFederate X.509 Certificate Integration Kit *User Guide*
Version 1.1
September, 2013

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Ping Identity, the Ping Identity logo, PingFederate, and the PingFederate icon are trademarks or registered trademarks of Ping Identity Corporation.

All other trademarks or registered trademarks are the properties of their respective owners.

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation does not provide any warranties and specifically disclaims any liability in connection with this document.

Contents

Introduction

The PingFederate X.509 Certificate Integration Kit provides an Identity Provider (IdP) Adapter that allows a PingFederate IdP server to perform client X.509 certificate authentication for single sign-on (SSO) to Service Provider (SP) applications.

The X.509 Certificate Adapter uses the PingFederate security infrastructure for certificate validation and management. PingFederate validates the trust of all certificates. A certificate is trusted if the root certificate of the issuing Certificate Authority (CA) is imported into the PingFederate trusted certificate store.

Using Object-Graph Navigation Language (OGNL) expressions, the Java X509Certificate object is available for mapping client certificate elements to attributes. For more information, see Sample OGNL Expressions on page 9.

Intended Audience

This document is intended for system administrators with some knowledge of PingFederate. Knowledge of networking and user-management configuration is assumed. Please consult the documentation provided with your server tools if you encounter difficulties in areas not directly associated with PingFederate or the X.509 Certificate Integration Kit.

Additional Resources

Administrators may want to review SSO Integration Kits and Adapters in the PingFederate *Administrator's Manual.*

Note: If you encounter any difficulties with configuration or deployment, please look for help at the Ping Identity Support Center (`www.pingidentity.com/support`).

System Requirements

The following prerequisites must be met to implement this Kit:

PingFederate 4.1 or higher

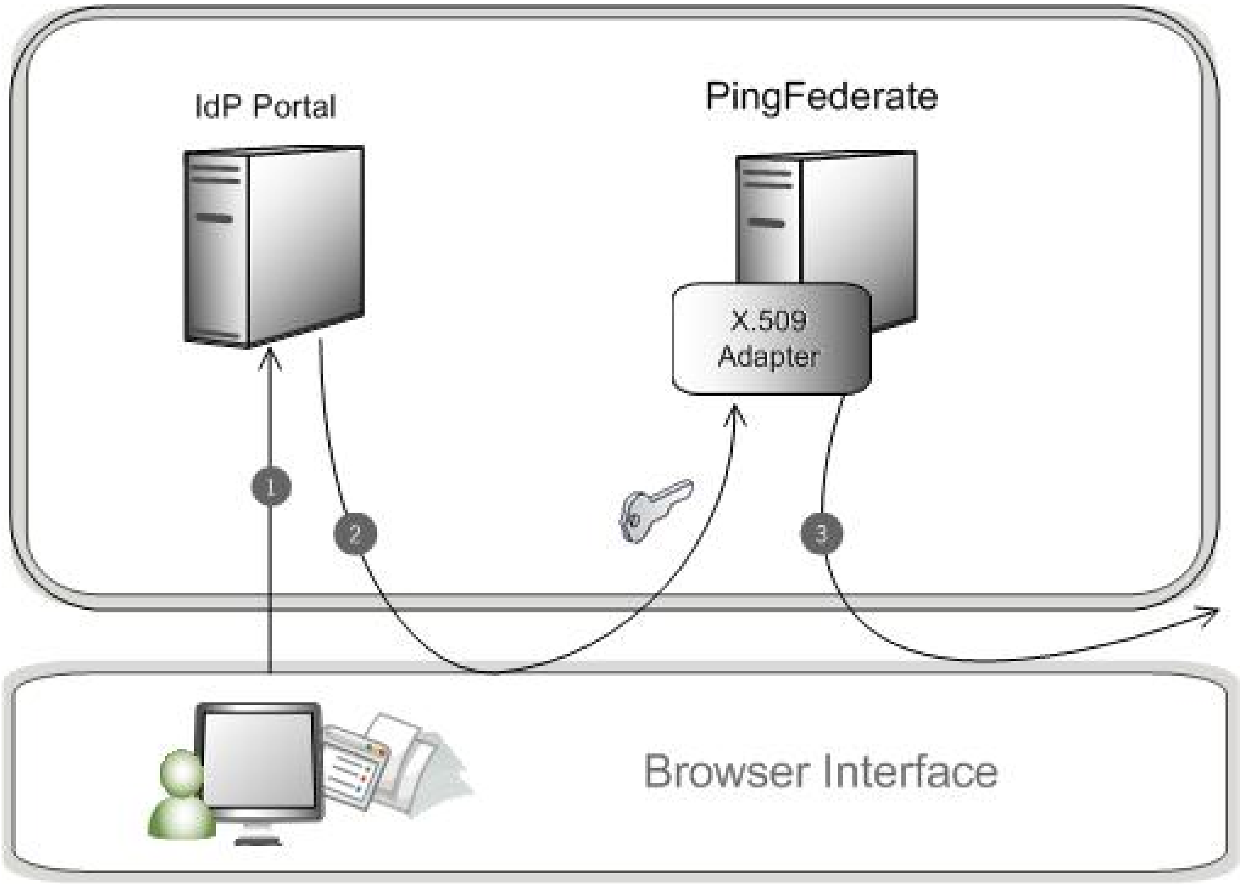
ZIP Manifest

The distribution ZIP file for the Integration Kit contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/dist` – contains libraries needed to run the Adapter
  - `X509-certificate-adapter-1.1.jar` – the X.509 Certificate Adapter JAR file

SSO Processing

The following figure shows a basic SSO scenario in which a PingFederate server authenticates users to an SP application using the X.509 Certificate Adapter.



Processing Steps

1. A user requests access to an SP resource from an IdP Internet Portal. The request is directed to PingFederate.
2. The browser requests the user’s client certificate. The PingFederate X.509 Certificate Adapter validates the certificate against a list of issuers. (If no issuers are specified in the Adapter setup, it uses the server’s list of trusted CAs instead.)
3. If the certificate is accepted, PingFederate creates a SAML assertion for the user for SSO to the requested partner SP site. (If the certificate is invalid, the user is taken to an error-page template.)

Installation and Setup

This section describes how to install and configure the X.509 Certificate Adapter.

1. Copy the `x509-certificate-adapter-1.1.jar` file from the `dist` directory of the distribution ZIP file to the `<pf-install>/pingfederate/server/default/deploy` directory of your PingFederate server installation.

2. In the `<pf-install>/pingfederate/bin` directory, open the file `run.properties` and change the value of `pf.secondary.https.port` from `-1` to a valid port number.

3. For PingFederate versions prior to 6.9, open the file `jboss-service.xml` located in the directory `<pf-install>/pingfederate/server/default/deploy/jetty.sar/META-INF.`

   Find the section titled "Add a second HTTPS/SSL Connector" and ensure the value of `WantClientAuth` is set to `true`, as shown below:

   ```
   <Set name="WantClientAuth">true</Set>
   ```

   Note: This value is set to `true` by default in PingFederate versions 6.0 and higher. For versions 6.9 and higher, the setting is also `true` out of the box, but the configuration file was changed and moved: you can verify the value by searching for `pf.secondary.https.port` in the file `jetty-runtime.xml` located in `<pf-install>/pingfederate/etc`.

   `WantClientAuth` causes the browser to redirect to a PingFederate error page if the client certificate is invalid. `NeedClientAuth` results in a browser error message instead of the PingFederate error page if the certificate is invalid.

4. Start or restart PingFederate.

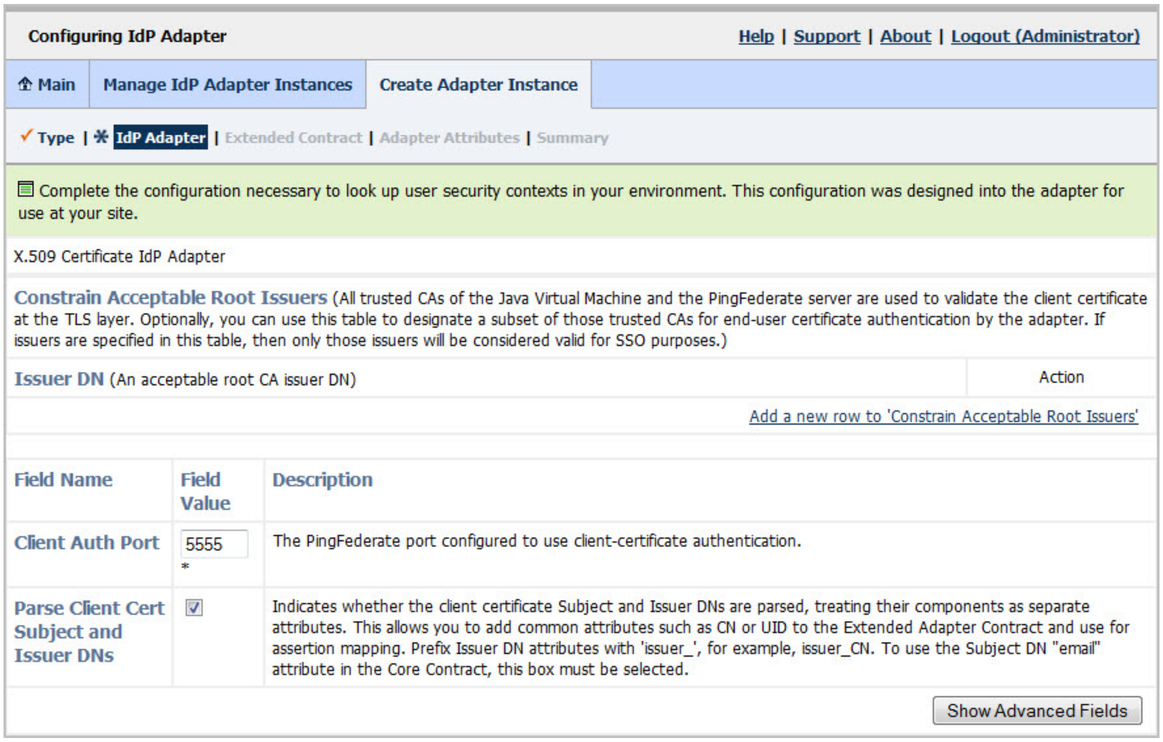
5. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.

6. On the Manage IdP Adapter Instances screen, click **Create New Instance**.

7. On the Type screen, enter an Instance Name and Instance Id.

   The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

8. Select X.509 Certificate IdP Adapter 1.1 from the Type list and click **Next**.



Configuring IdP Adapter

Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Type | ✱ IdP Adapter | Extended Contract | Adapter Attributes | Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

X.509 Certificate IdP Adapter

Constrain Acceptable Root Issuers (All trusted CAs of the Java Virtual Machine and the PingFederate server are used to validate the client certificate at the TLS layer. Optionally, you can use this table to designate a subset of those trusted CAs for end-user certificate authentication by the adapter. If issuers are specified in this table, then only those issuers will be considered valid for SSO purposes.)

Issuer DN (An acceptable root CA issuer DN)	Action
	Add a new row to 'Constrain Acceptable Root Issuers'

Field Name	Field Value	Description
Client Auth Port	5555 *	The PingFederate port configured to use client-certificate authentication.
Parse Client Cert Subject and Issuer DNs	☑	Indicates whether the client certificate Subject and Issuer DNs are parsed, treating their components as separate attributes. This allows you to add common attributes such as CN or UID to the Extended Adapter Contract and use for assertion mapping. Prefix Issuer DN attributes with 'issuer_', for example, issuer_CN. To use the Subject DN "email" attribute in the Core Contract, this box must be selected.

9. (Optional) Click **Add a new row to 'Constrain Acceptable Root Issuers'** under Action, enter an applicable CA Issuer DN, and click **Update**.

   Use this section to add a subset of certificates (issued by trusted root CAs) for end-user certificate authentication by the adapter. Client certificates are validated at the TLS layer against all trusted CAs of the Java Virtual Machine and the PingFederate server, but here you can further restrict which issuers are validated in the adapter instance for SSO.

   Repeat this step for any additional trusted CAs.

10. Enter the Client Auth Port specified for the `pf.secondary.https.port` (see step 2).

11. (Optional) Leave the Parse Client Cert Subject and Issuer DNs checkbox selected to parse the certificate Subject and Issuer DNs.

    Parsing the DNs makes the standard components available for the extended attribute contract. For example, you can map the CN element of the Subject DN to one attribute and map the CN element of the Issuer DN to a different attribute. The Subject DN email component is also available as part of the Core Contract on the next screen.

Note: If you want to extract other components of the X.509 client certificate, use OGNL expressions. For example expressions, see Sample OGNL Expressions on page 9.

Note: Neither Subject DN nor Issuer DN elements are available for the extended contract or OGNL processing if you clear this box.

12. (Optional) Click **Show Advanced Fields**.

    The Return Success on SLO option is provided for continuity of single-logout events among SP partners through this adapter (which does not itself support SLO). If your federation deployment does not require SLO, this option has no effect. If your deployment does require SLO, we recommend that you keep the option selected.

For more information about SLO processing, see Supported Standards in *Getting Started*.

13. Click **Next**.

14. (Optional) On the Extended Contract screen, add any Subject DN or Issuer DN components you want to send individually in the SAML assertion, in addition to the full DNs.

    Note: The DN components are available separately only if the Parse Client Cert Subject and Issuer DNs checkbox is selected (the default) on the IdP Adapter screen. The core attribute Subject DN email is also available, but only if the checkbox is selected.

    The attributes you enter must be in uppercase. Only attributes specified in RFC 2253 are allowed (CN, L, ST, O, OU, C, STREET, DC, and UID). Issuer attributes require a prefix of issuer_ before the attribute—for example, issuer_CN.

15. On the Adapter Attributes screen, indicate at least one attribute to be used as a Pseudonym.

    Optionally, you can also choose to obfuscate any of the attributes in PingFederate log files.

    For more information about these features, see Managing Log Files and Account Linking in the PingFederate *Administrator's Manual* or refer to the context-sensitive **Help** page.

16. On the Summary screen, click **Done**.

Testing the Adapter

You can test the configuration using the IdP Quick-Start Applications that ship with PingFederate 5.x-6.2. (For version 4.x, these are called "Sample Applications.") For PingFederate versions 6.3 and later, the Quick-Start Applications are available from the Ping Identity download site (www.pingidentity.com/support-and-downloads).

Note: You need a client certificate to test the adapter. If the certificate is self-signed or issued by a CA not in the Java Virtual Machine trust store, it must be imported into the PingFederate trusted store (see Trusted Certificate Authorities in the PingFederate *Administrator's Manual*).

Follow this procedure to test your adapter configuration:

1. Set up PingFederate to run the SP Application according to instructions in the *Quick-Start Guide*.

2. Reconfigure the SP sample connection to use the X.509 Certificate Adapter instance (see Installation and Setup on page 4).

   Delete the existing adapter instance and map the X.509 Certificate Adapter instance in its place. (See IdP Adapter Mapping in the PingFederate *Administrator's Manual* or the online **Help** pages for detailed information.)

3. In a real application, there would be a link or a redirect to a PingFederate application endpoint to initiate the SSO. Since this is just a test, go to the following URL directly in the browser:

   ```
   https://<PF_host>:<ssl_port>/idp/startSSO.ping?PartnerSpId=<connection_id>
   ```

where:

- `<PF_host>` is the domain name (or IP address) of the machine running the PingFederate server (default value: `localhost`).
- `<ssl_port>` is the PingFederate SSL port (default value: `9031`).
- `<connection_id>` is the Connection ID of the SP connection. For PingFederate 4.x, the value is `localhost:default:entityId`; for 5.x, the value is `PF-DEMO`.

4. Select your client certificate. If the certificate is validated, you are logged on to the Quick-Start/Sample SP Application.

Sample OGNL Expressions

Client certificates are available as `java.security.cert.X509Certificate` objects, making the methods available for mapping certificate attributes. These methods are defined in the Java Platform, Standard Edition API Specification. For a full list of available methods, see the J2SE online javadoc.

To retrieve the first client certificate in the chain as an X509Certificate object, you must use the `ClientCertificateChain` keyword within the OGNL expression. For example:

```
#this.get("ClientCertificateChain").getObjectValue()
```

To retrieve the entire client certificate chain as an iterable collection of X509Certificate objects, use the `getAllObjectValues()` method in the OGNL expression. For example:

```
#this.get("ClientCertificateChain").getAllObjectValues()
```

The following table lists sample OGNL expressions administrators might use when mapping certificate attributes during the setup or deployment of the X.509 Certificate Adapter. For information about using OGNL for attribute mapping in PingFederate, see Using Attribute Mapping Expressions in the PingFederate *Administrator's Manual*.

OGNL Expression	Description
`#x509Cert = #this.get("ClientCertificateChain").getObjectValue(), #hexEncoded = new String(@org.apache.commons.codec.binary.Hex@encodeHex(#x509Cert.getSignature()))`	Returns a hex-encoded signature from the X.509 client certificate.
`#x509Cert = #this.get("ClientCertificateChain").getObjectValue(), #hexEncoded = new String(@org.apache.commons.codec.binary.Hex@encodeHex(#x509Cert.getExtensionValue("2.16.840.1.113730.1.13")))`	Extracts the comment certificate extension (Object Identifier (OID) 2.16.840.1.113730.1.13) from the X.509 client certificate, which is then hex encoded. Other certificate extensions can be extracted by using the correct OID for the extension.