Single Sign-On with SAML 2.0 and ABAP Systems Supporting SAP Logon Tickets

Created by Desislava Petkova on Mar 27, 2017

This wiki page describes implementing a single sign-on mechanism with SAML 2.0 in a network including an ABAP system which does not support SAML 2.0 authentication. Explanations are based on a sample real-life scenario.

In summary, you need the following products to try out this scenario:

- SAP NetWeaver Application Server Java 7.2/7.3 (the service provider in the scenario)
- An identity provider, such as SAP NetWeaver Identity Management 7.2 or SAP NetWeaver Single Sign-On or another vendor's identity provider
- An ABAP system, such as SAP NetWeaver Application Server ABAP 7.0 or 6.40 or system which supports SAP logon tickets (MYSAPSSO2 Cookie, SSO2 Tickets).

Table of contents

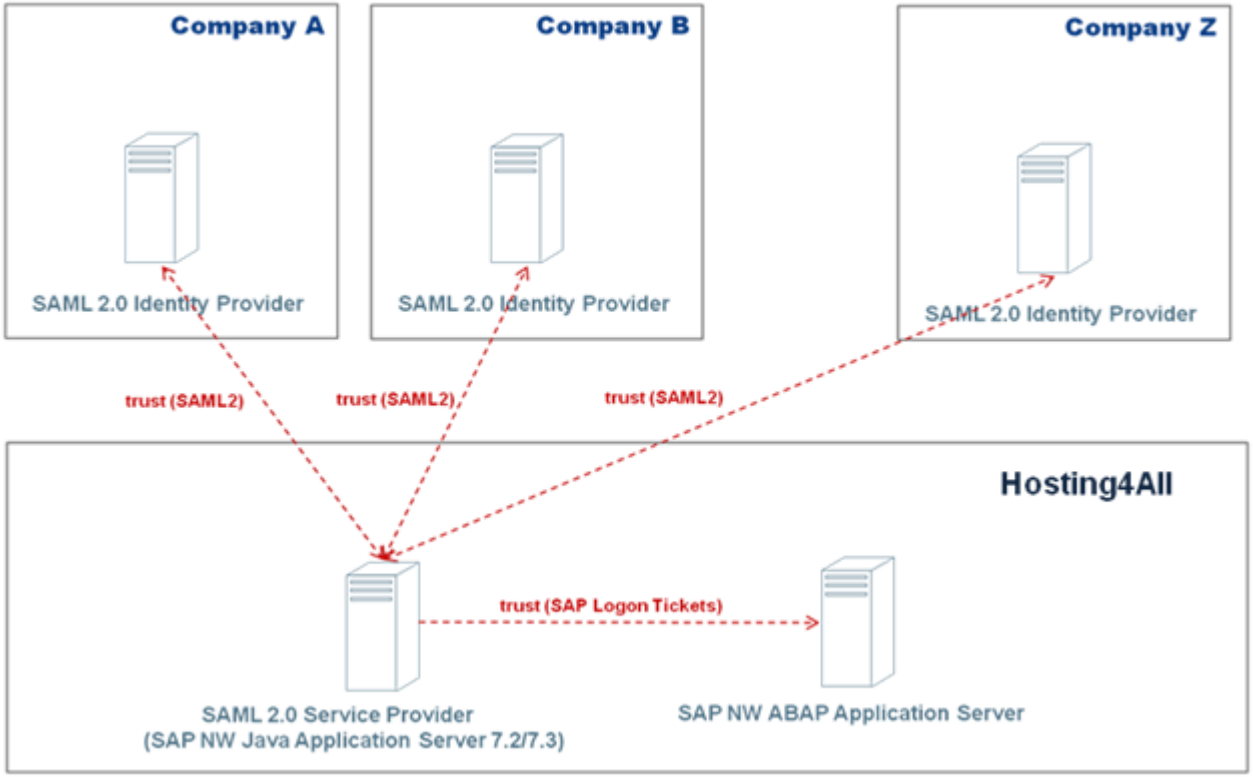
Scenario Description

Hosting company "Hosting4All" hosts products/applications for a number of customers – the companies A, B,… , Z. These applications run on an ABAP system. Each customer uses a separate ABAP client so that there is isolation between companies' data.

Users from different companies have accounts at the ABAP system and can log in with username and password. However, "Hosting4All" would like to make the users' life easier by introducing Single Sign-On to the ABAP system. This would prevent users from having to re-enter username and password for accessing each separate application.

"Hosting4All" decides to introduce SAML 2.0 authentication and in this way achieve single sign-on to the ABAP system. Each company A, B, …, Z already has a SAML 2.0 identity provider ready to authenticate the users from this company. Users from companies A, B, …, Z do not have accounts on the SAML 2.0 service

provider system of “Hosting4All” and customer companies do not want to provision the accounts. Users from companies A, B, …, Z only have accounts on the ABAP system and identity provider is aware of these accounts.



To achieve its goal, “Hosting4All” needs to have SAP NetWeaver Application Server Java 7.2/7.3 with the necessary configuration.

eLearnings Containing All the Steps

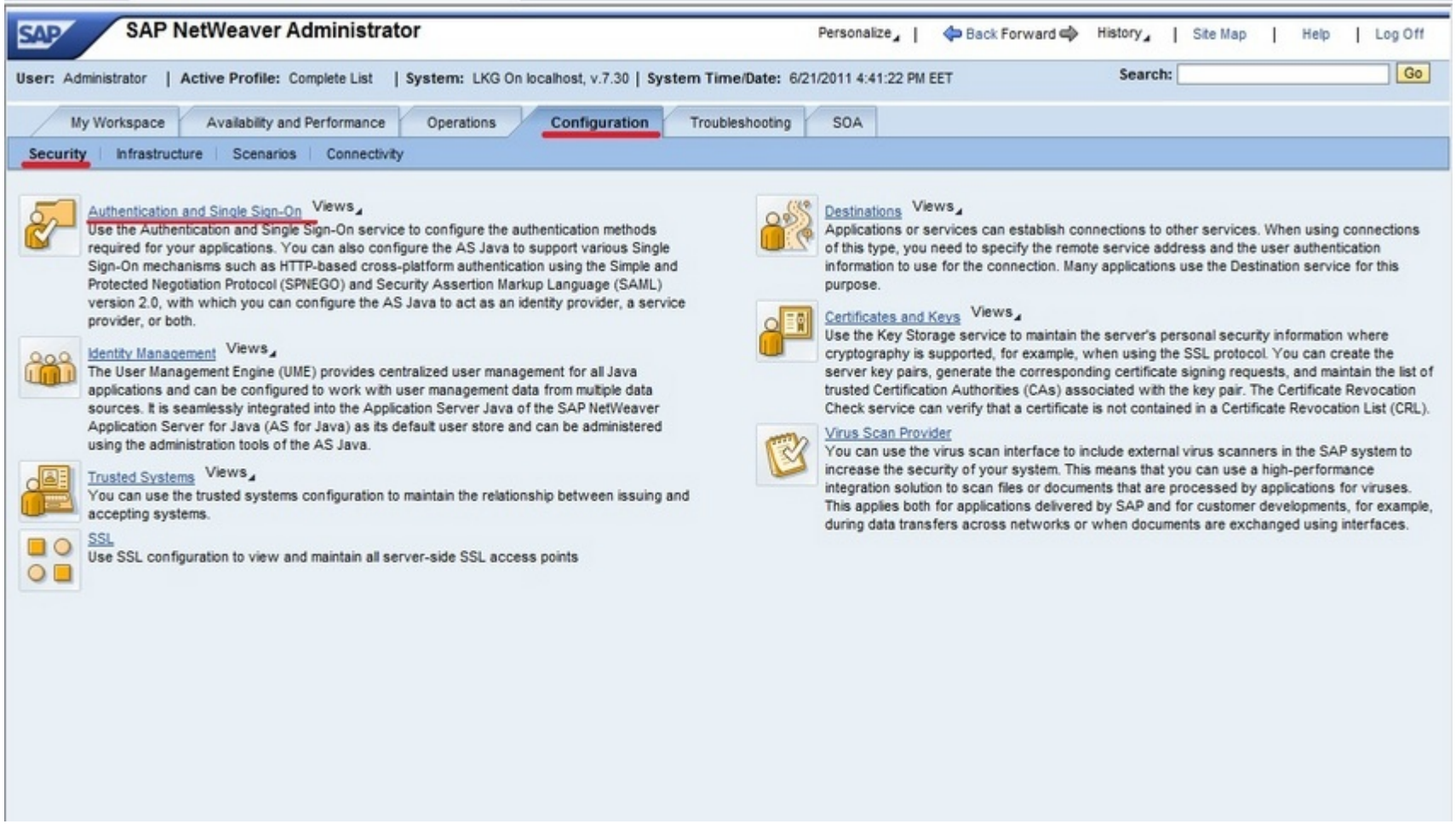
All the steps described in this wiki page are also available as video tutorials in the eLearning area:

Configuring the SAML 2.0 Service Provider
Configuring a SAML 2.0 Identity Provider
Configuring Trust on the Identity Provider Side
Configuring Trust on the Service Provider Side
Exporting the SAP Logon Ticket
Using Single Sign-On

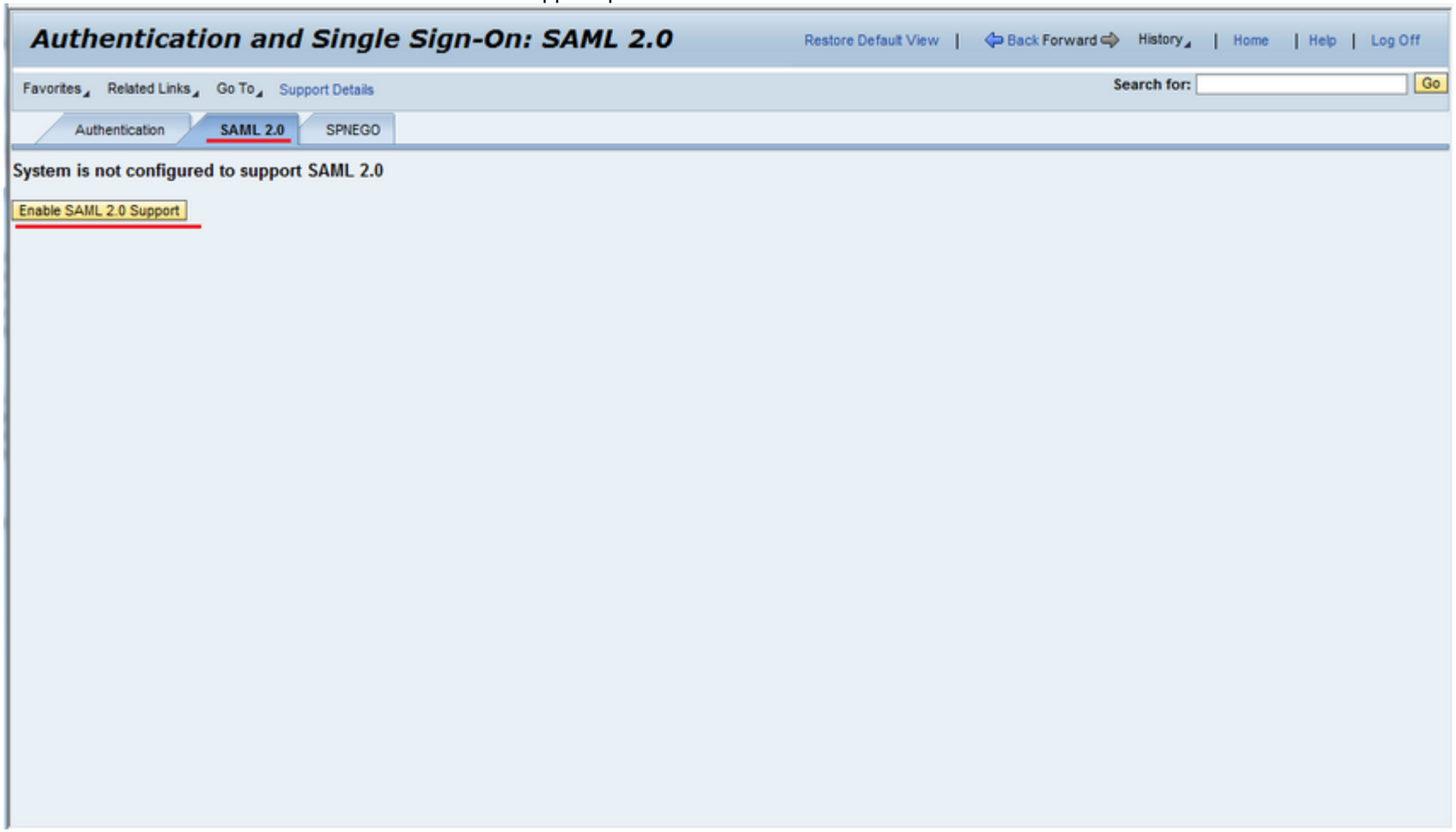
Creating SAML 2.0 Service Provider on “Hosting4All”

Video tutorial with the steps: Configuring the SAML 2.0 Service Provider
The steps below describe the creation and initial configuration of SAML 2.0 service provider.

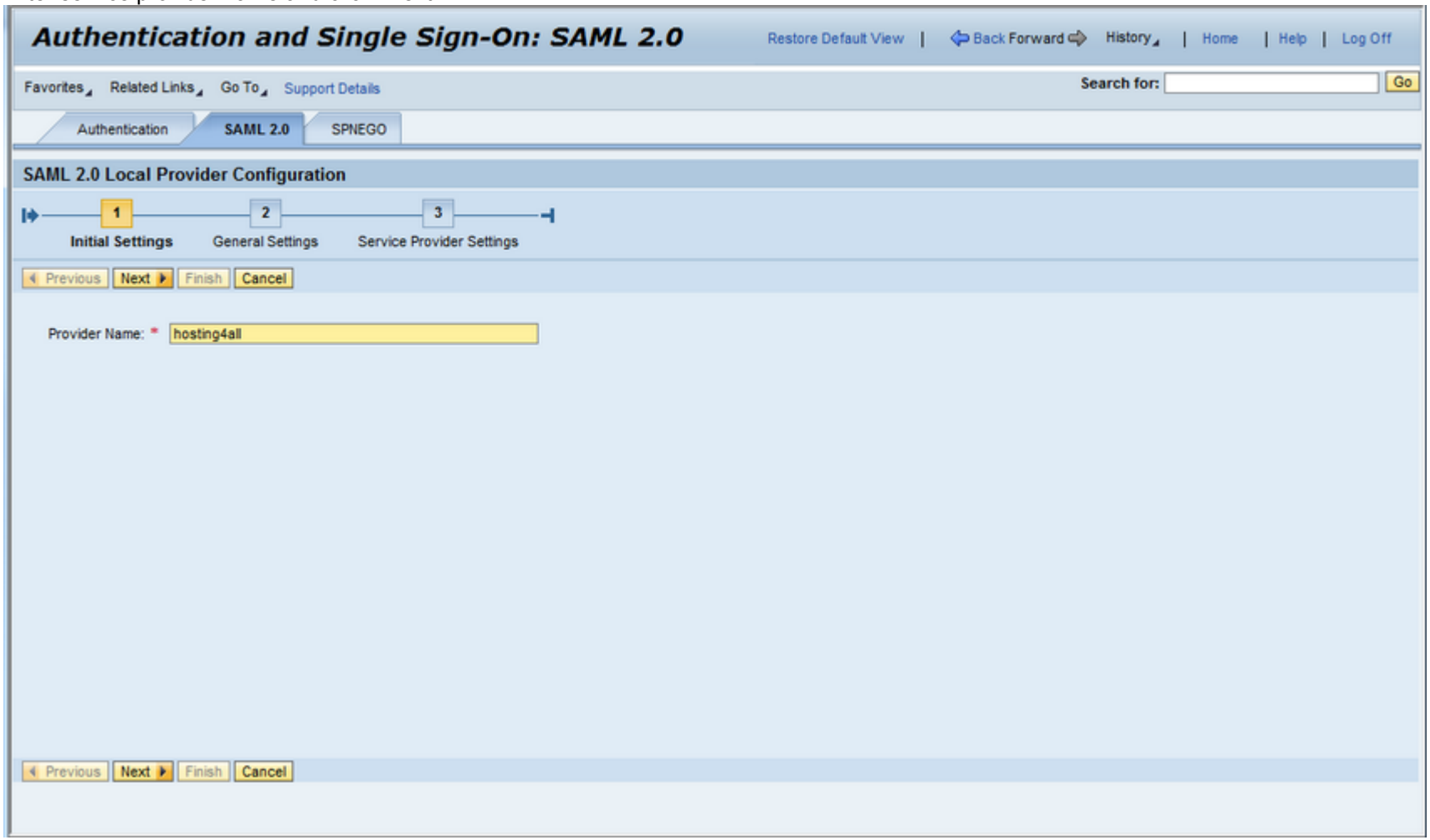
1. Open http(s)://<java server host>:<port>/nwa -> Configuration -> Authentication and Single Sign-On



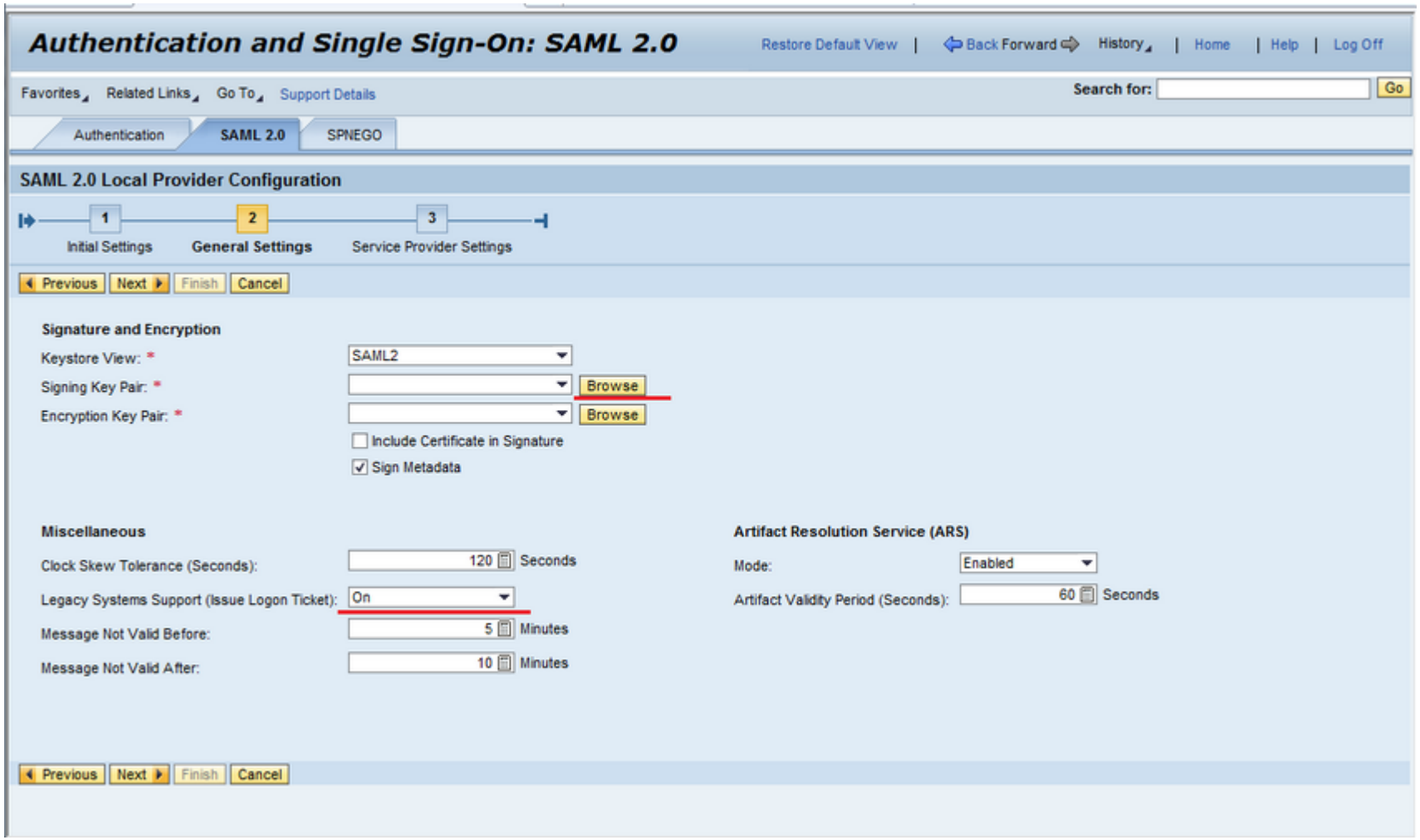
2. Select “SAML 2.0” tab and click “Enable SAML 2.0 Support” pushbutton.



3. Enter service provider name and click "Next".

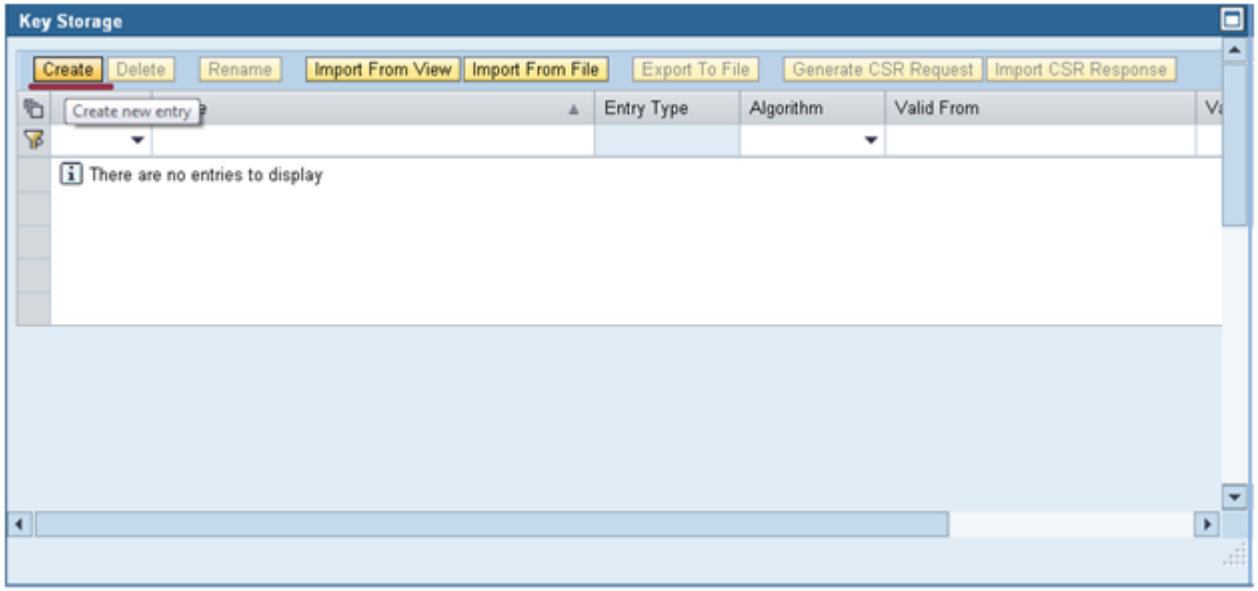


4. Change setting “Legacy Systems Support (Issue Logon Ticket)” to “On”
   Having legacy system support setting set to “On” means that service provider will issue SAP Logon ticket which could be consumed later by the ABAP system. More information can be found at help.sap.com .
5. Now you need a signing key pair for the local provider. It will be used as encryption key pair as well. To create service provider key pair, click the "Browse" button next to the "Signing Key Pair" field.

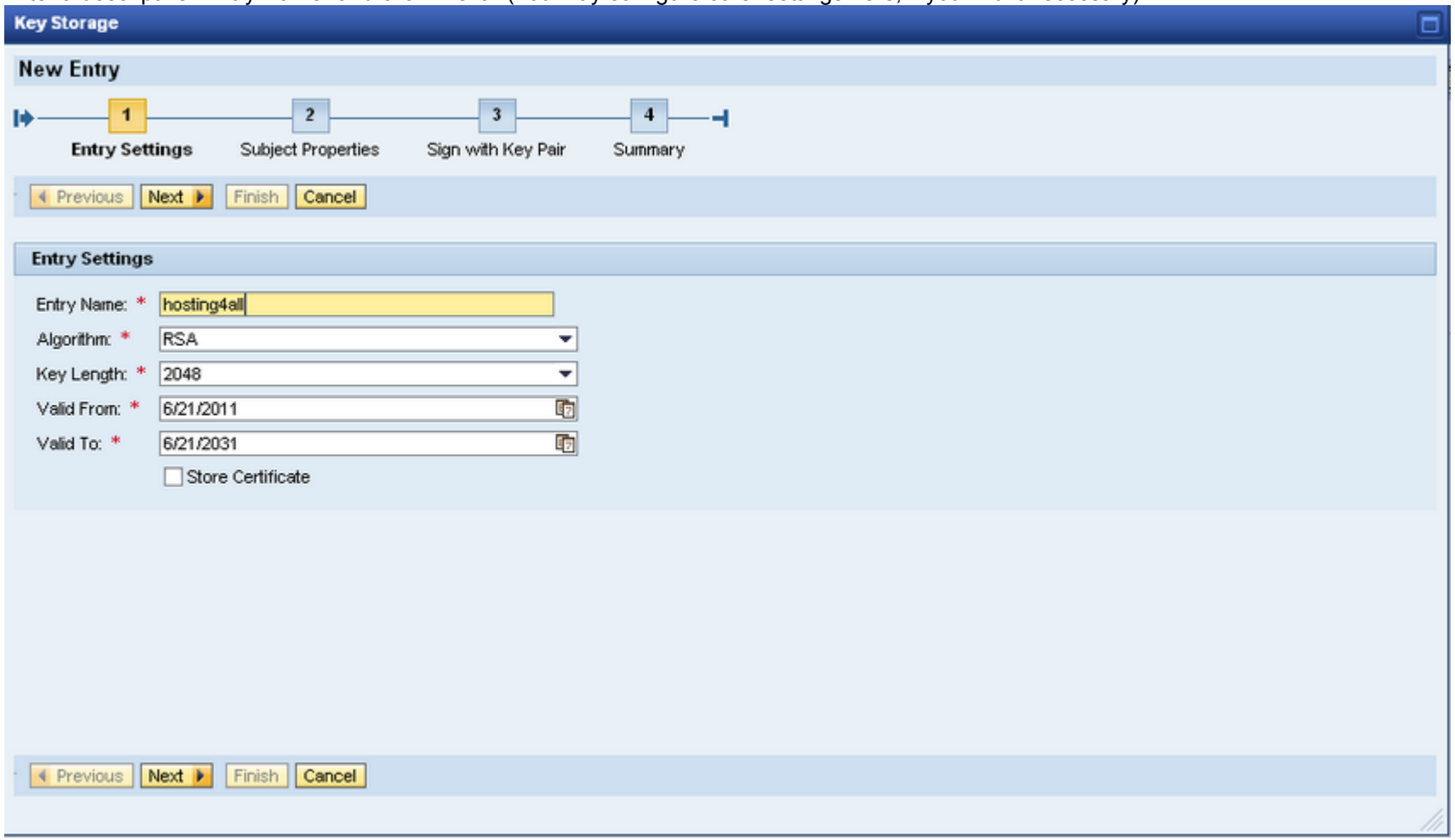


The key storage opens.
Here are the steps for creating the key pair:

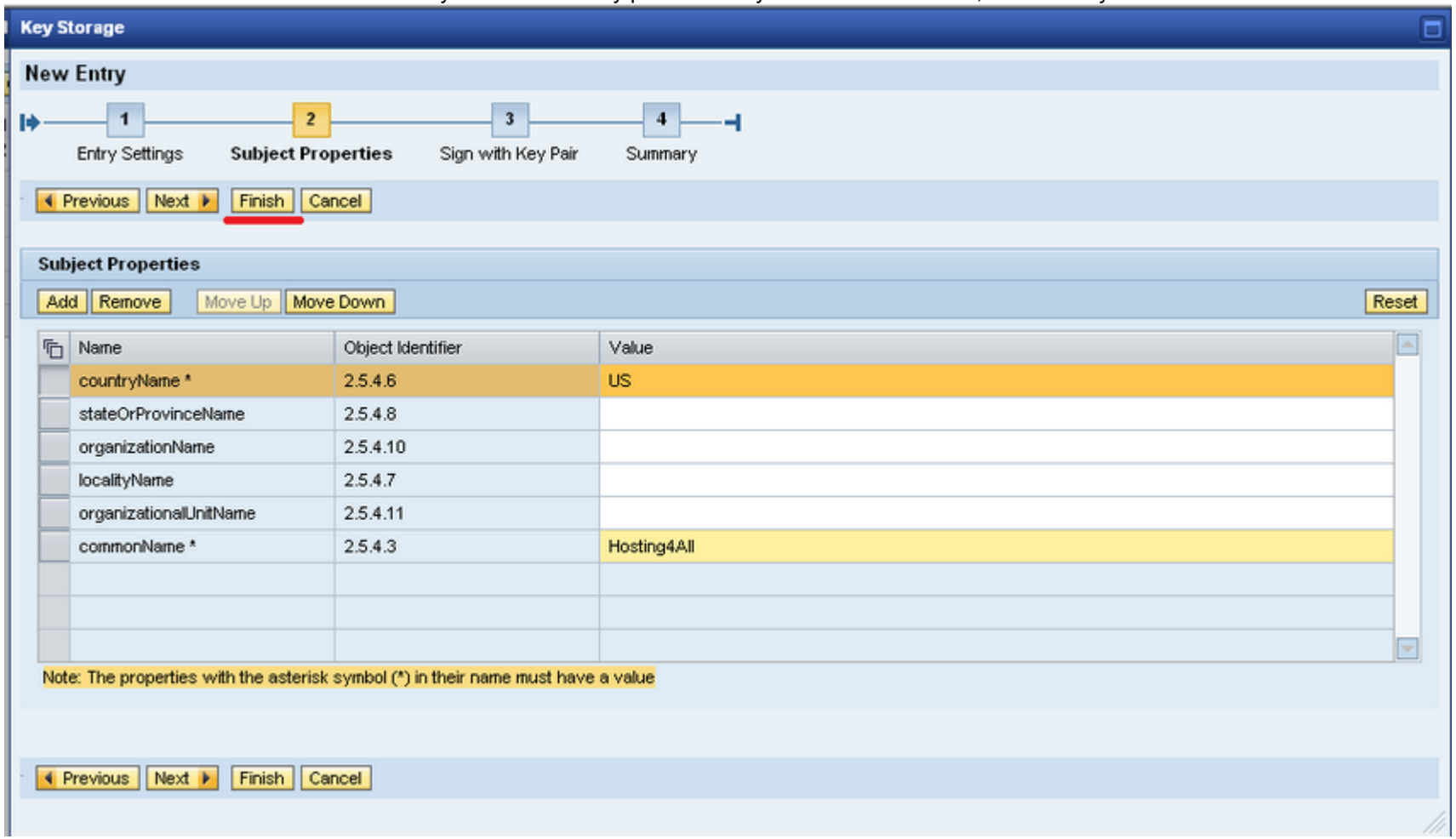
a. Click "Create".



b. Enter a descriptive "Entry Name" and click "Next". (You may configure other settings here, if you find it necessary).

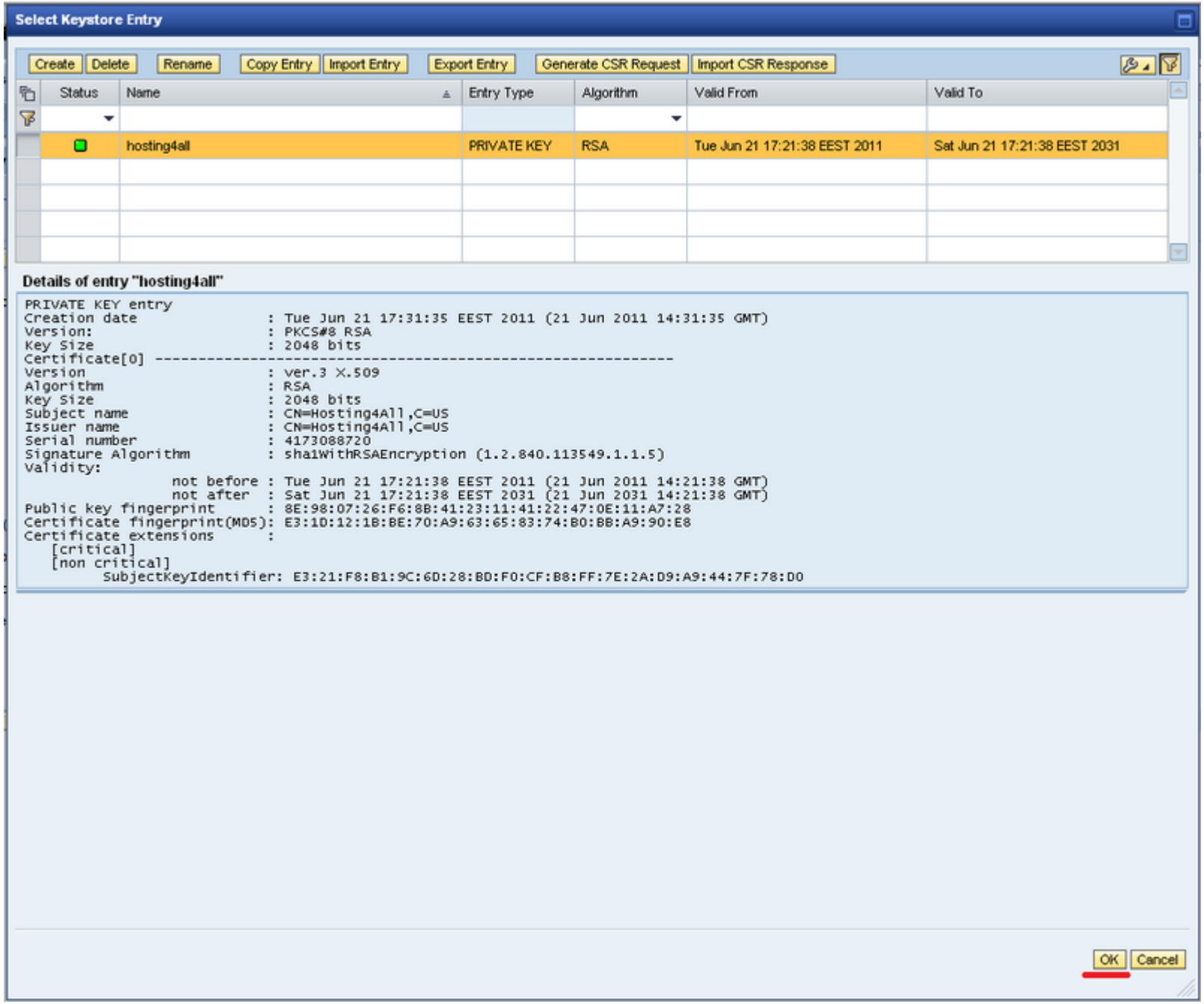


c. Enter at least the commonName and countryName for the key pair. You may also add other fields, if necessary. Click "Finish".

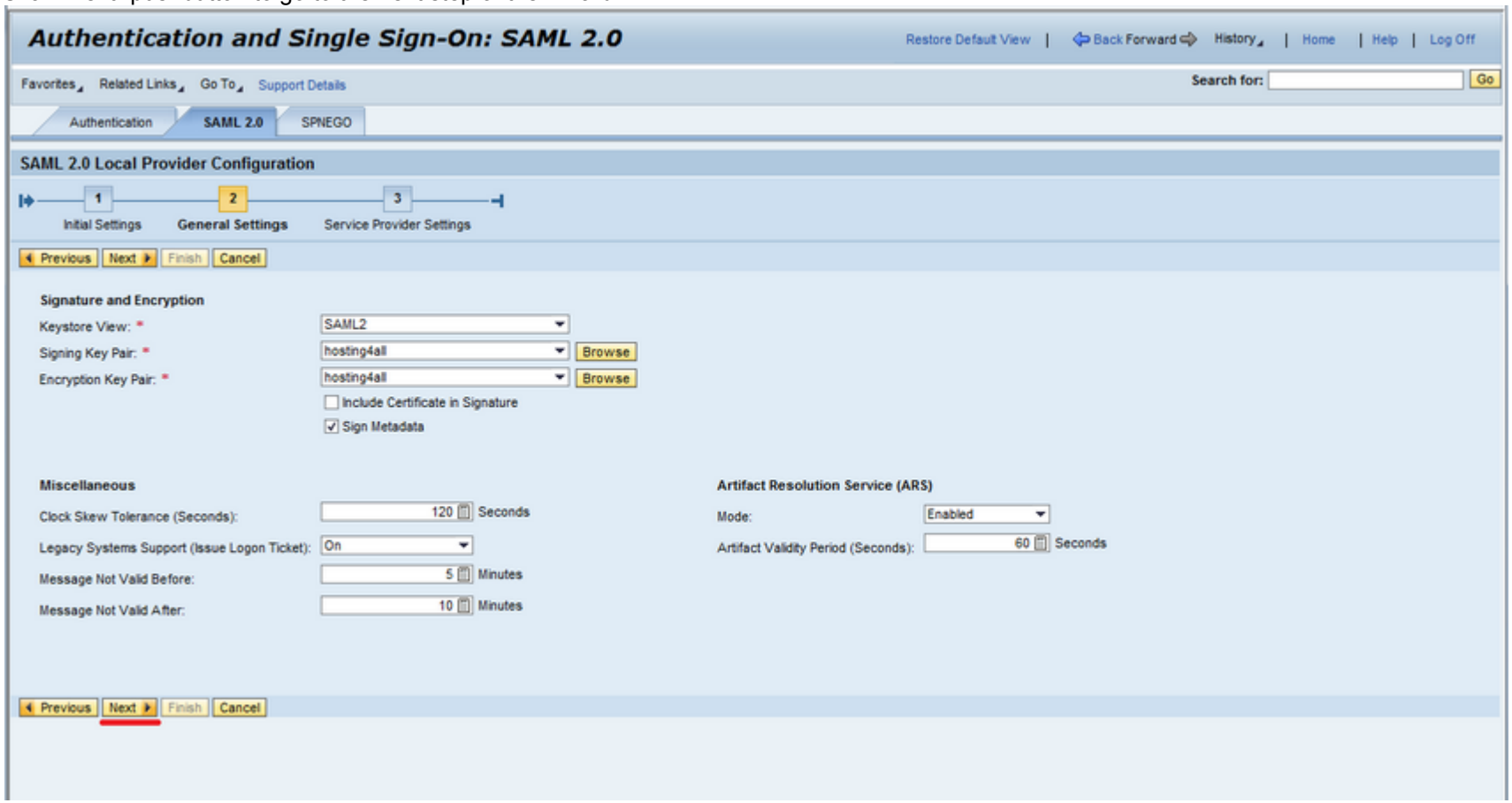


The details of the created key pair are displayed.

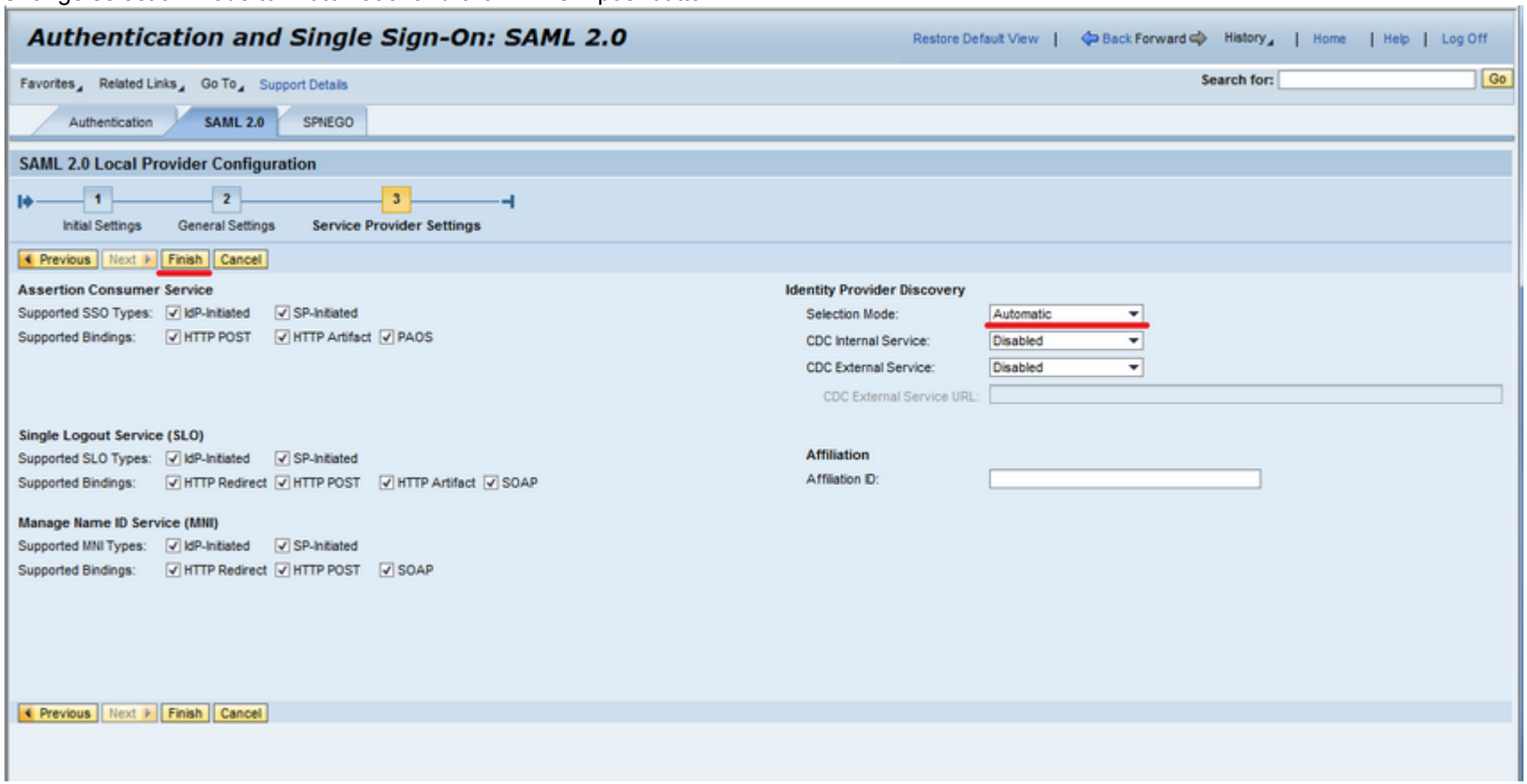
d. Click "OK".


Select Keystore Entry
Create
Delete
Rename
Copy Entry
Import Entry
Export Entry
Generate CSR Request
Import CSR Response
Status
Name
Entry Type
Algorithm
Valid From
Valid To
hosting4all
PRIVATE KEY
RSA
Tue Jun 21 17:21:38 EEST 2011
Sat Jun 21 17:21:38 EEST 2031
Details of entry "hosting4all"
PRIVATE KEY entry
Creation date : Tue Jun 21 17:31:35 EEST 2011 (21 Jun 2011 14:31:35 GMT)
Version: : PKCS#8 RSA
Key Size : 2048 bits
Certificate[0] ----------
Version : ver.3 X.509
Algorithm : RSA
Key Size : 2048 bits
Subject name : CN=Hosting4All,C=US
Issuer name : CN=Hosting4All,C=US
Serial number : 4173088720
Signature Algorithm : sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Validity:
not before : Tue Jun 21 17:21:38 EEST 2011 (21 Jun 2011 14:21:38 GMT)
not after : Sat Jun 21 17:21:38 EEST 2031 (21 Jun 2031 14:21:38 GMT)
Public key fingerprint : 8E:98:07:26:F6:8B:41:23:11:41:22:47:0E:11:A7:28
Certificate fingerprint(MD5): E3:1D:12:1B:BE:70:A9:63:65:83:74:B0:BB:A9:90:E8
Certificate extensions :
[critical]
[non critical]
SubjectKeyIdentifier: E3:21:F8:B1:9C:6D:28:BD:F0:CF:B8:FF:7E:2A:D9:A9:44:7F:78:D0
OK
Cancel

6. Click "Next" pushbutton to go to the next step of the wizard:

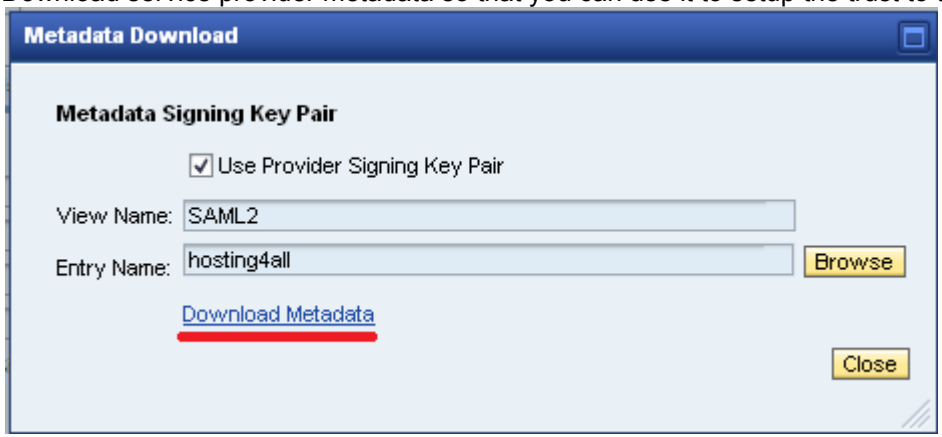


7. Change selection mode to “Automatic” and click “Finish” pushbutton:

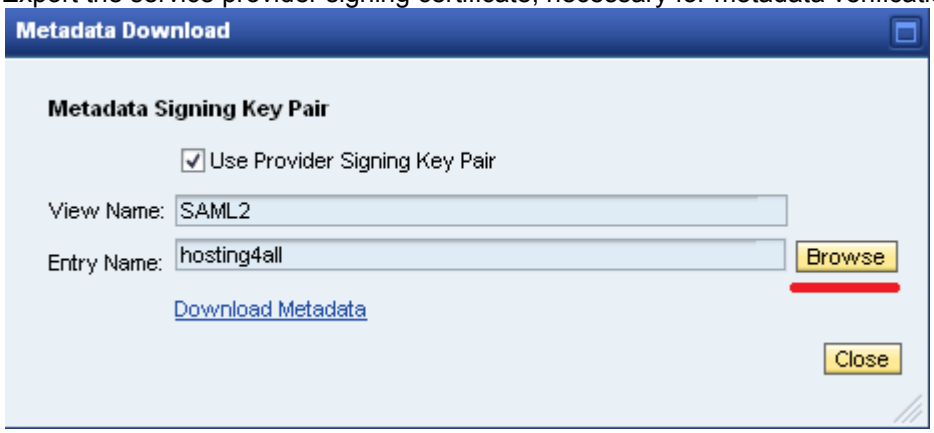


More information regarding identity provider discovery settings can be found at help.sap.com .

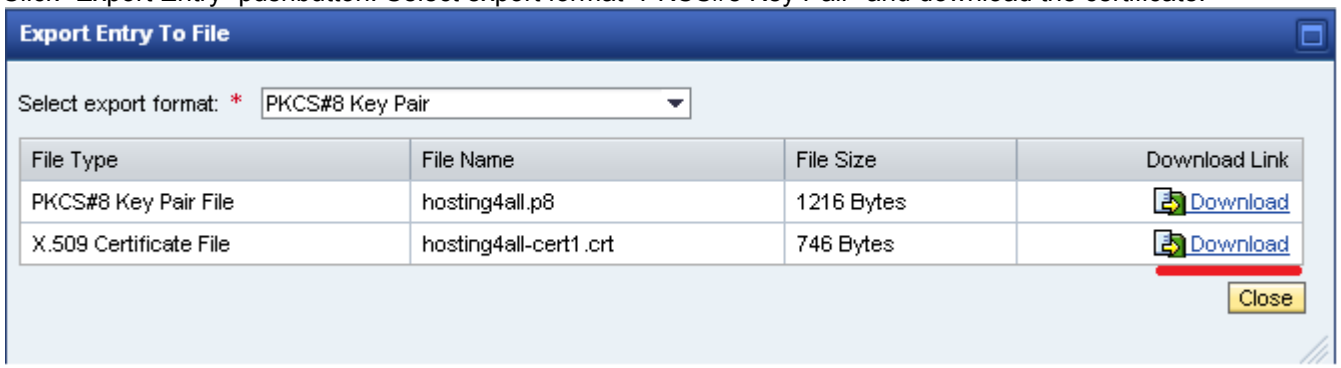
8. Download service provider metadata so that you can use it to setup the trust to the service provider at identity provider side.



9. Export the service provider signing certificate, necessary for metadata verification at identity provider side



10. Click “Export Entry” pushbutton. Select export format “PKCS#8 Key Pair” and download the certificate:



More information regarding metadata access can be found at help.sap.com
Send the identity provider both the metadata file and the exported certificate so that trust between identity provider and service provider can be configured.

Creating SAML 2.0 Identity Provider

To setup the scenario, any SAML 2.0 identity provider can be used.
For more information how to setup SAP-vendored identity provider see video Configuring a SAML 2.0 Identity Provider

Configuring Trust on the SAML 2.0 Identity Provider Side

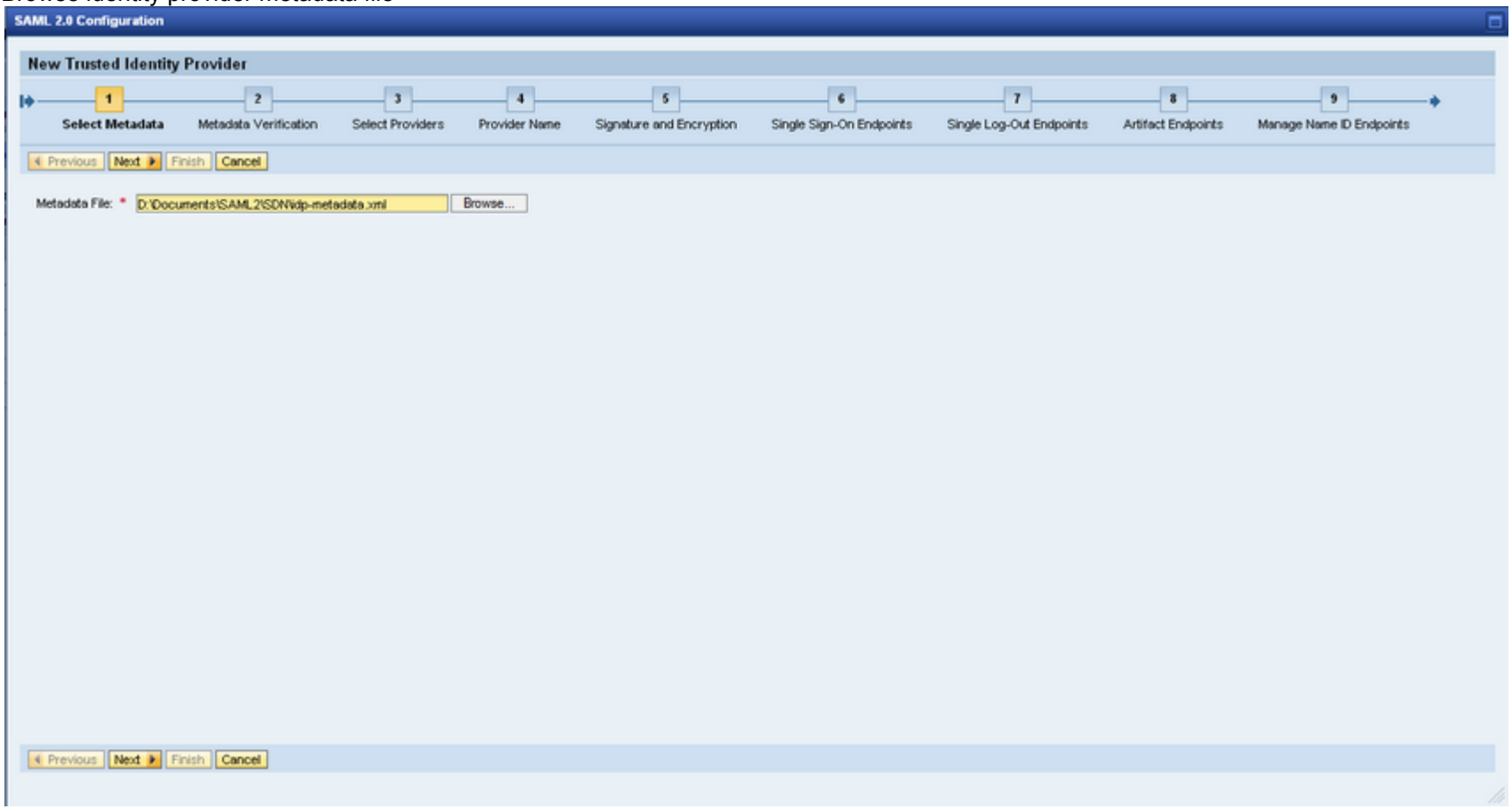
In this step, you need to configure the identity provider to trust the service provider. For SAP-vendored identity provider see video Configuring Trust on the Identity Provider Side

Configuring Trust on the SAML 2.0 Service Provider Side

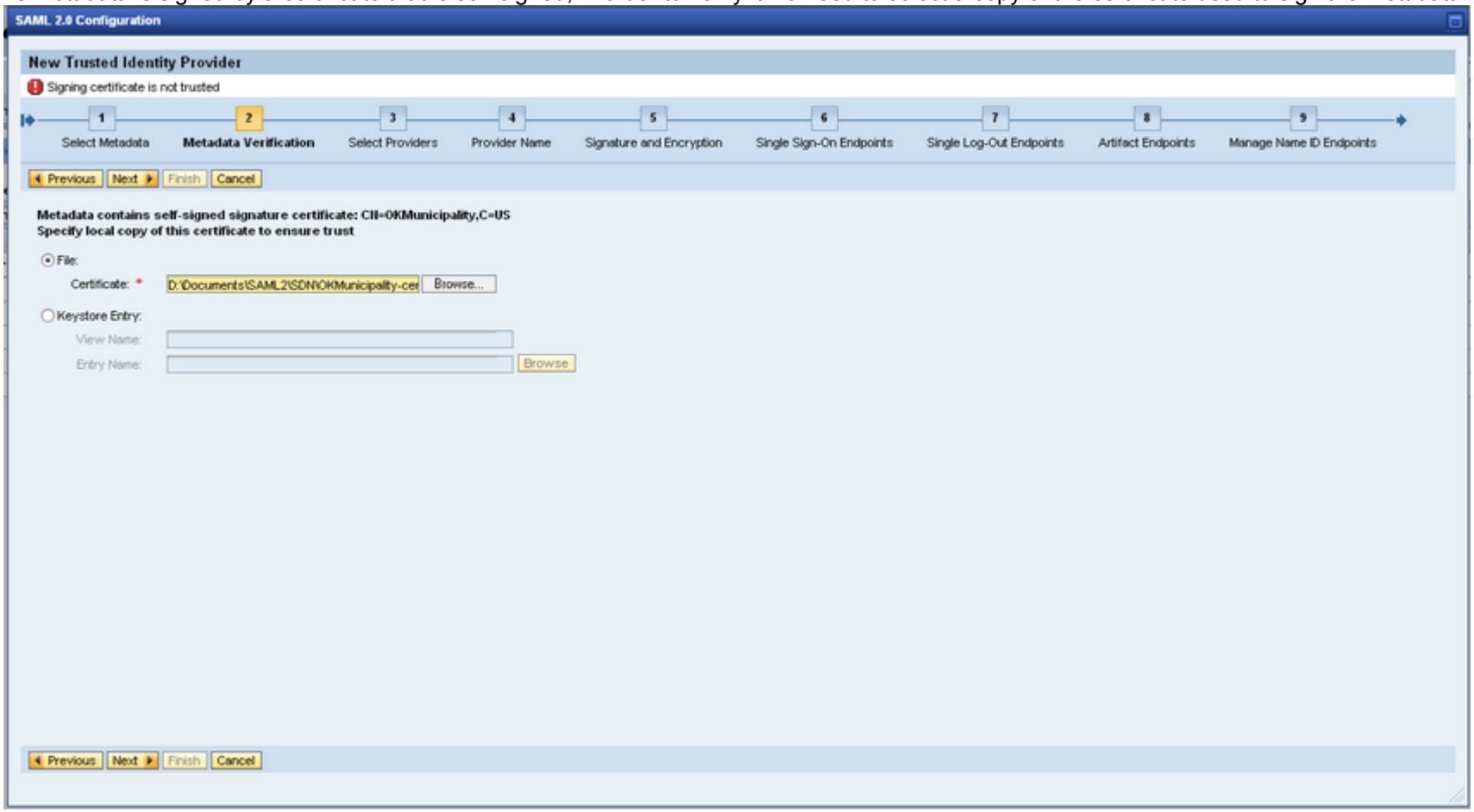
Video tutorial with the steps: Configuring Trust on the Service Provider Side
The steps below describe the configuration between the SAML 2.0 service provider of “Hosting4All”, and the SAML 2.0 identity provider of a customer, for example company A.

Prerequisite
You have received SAML 2.0 metadata and signing certificate from identity provider.

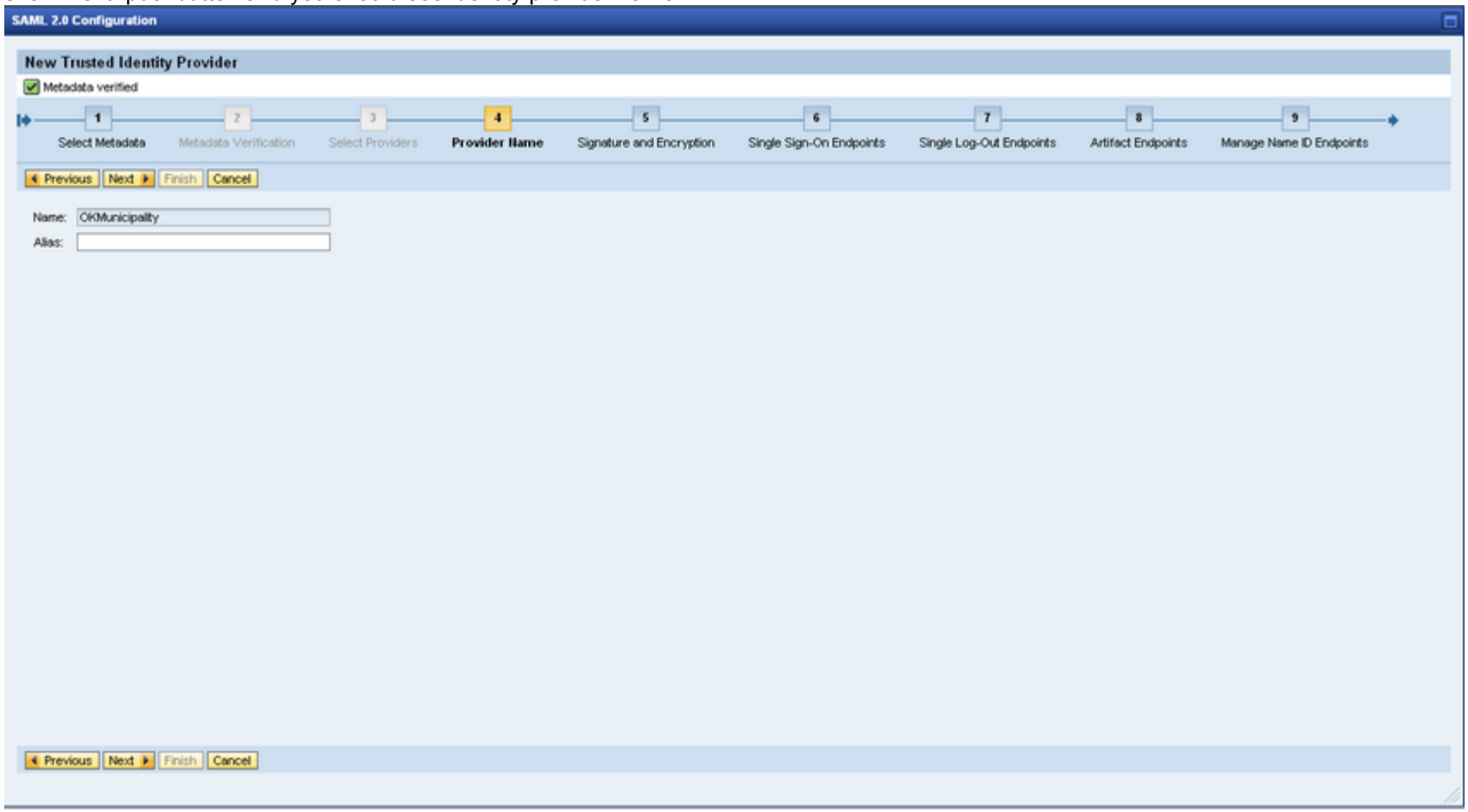
1. Open http(s)://<java server host>:<port>/nwa -> Configuration -> Authentication and Single Sign-On. Select “SAML 2.0” tab and go to “Trusted Providers” link. Click “Add” pushbutton and choose “Uploading Metadata File”
2. Browse identity provider metadata file



3. As metadata is signed by a certificate that is self-signed, in order to verify it we need to select a copy of the certificate used to sign the metadata



4. Click “Next” pushbutton and you should see identity provider name



5. Just go through the wizard by leaving the default values. At the last step click "Finish" pushbutton and the new trusted identity provider will be created.

   More information on trusting an identity provider can be found at help.sap.com

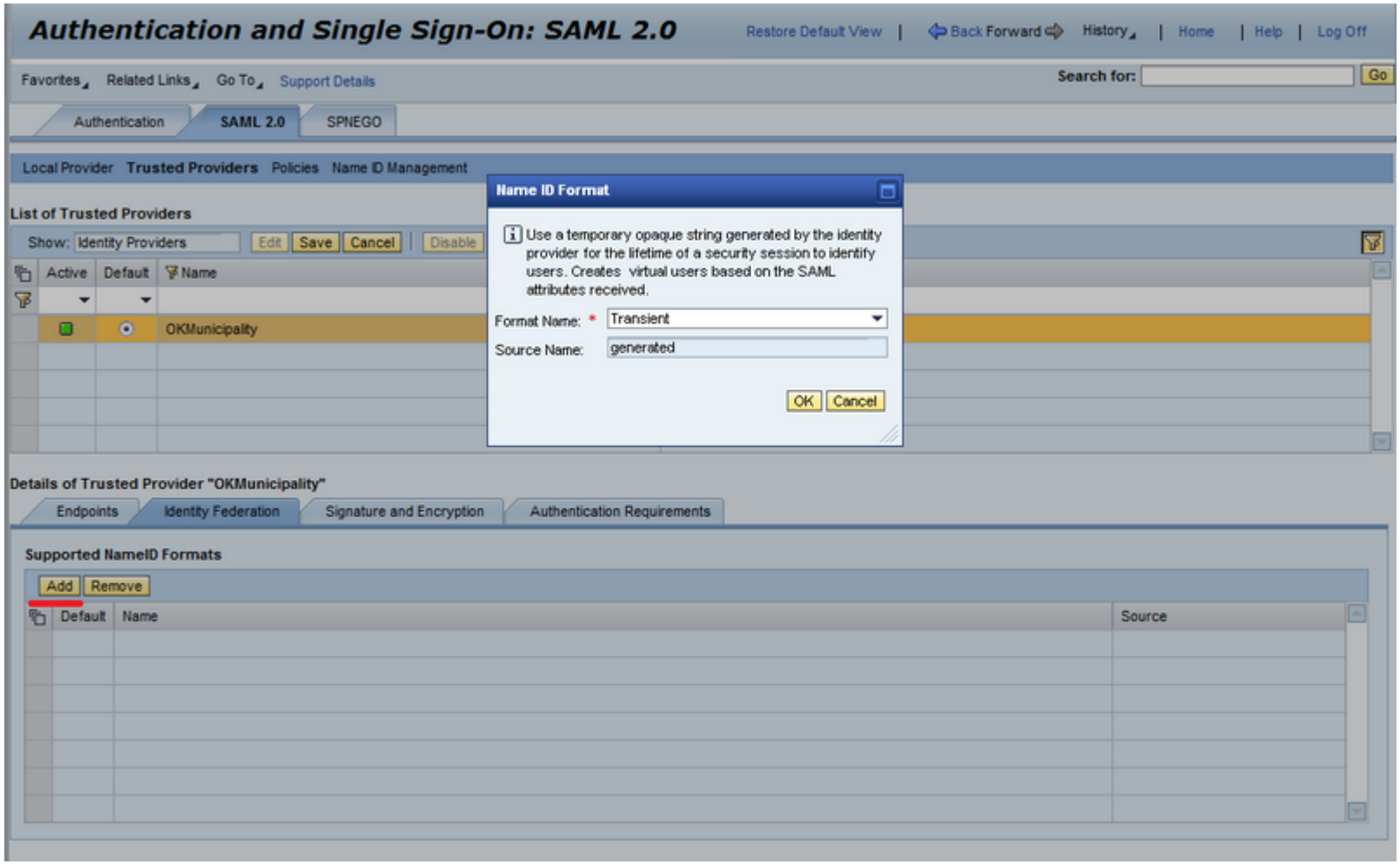
Configuring Identity Federation on SAML 2.0 Service Provider of "Hosting4All"

Configuration of identity federation is actually information which tells service provider how to interpret SAML 2.0 data coming from identity provider. Steps below describe how this configuration is done.

As users who are already authenticated at the customers’ identity providers do not have accounts on the service provider, in-memory users can be used for SAML 2.0 authentication at service provider. In-memory users are just like ordinary users (can have groups and roles) except for the fact that they do not have permanent accounts. In-memory users are deleted as soon as their session is terminated.

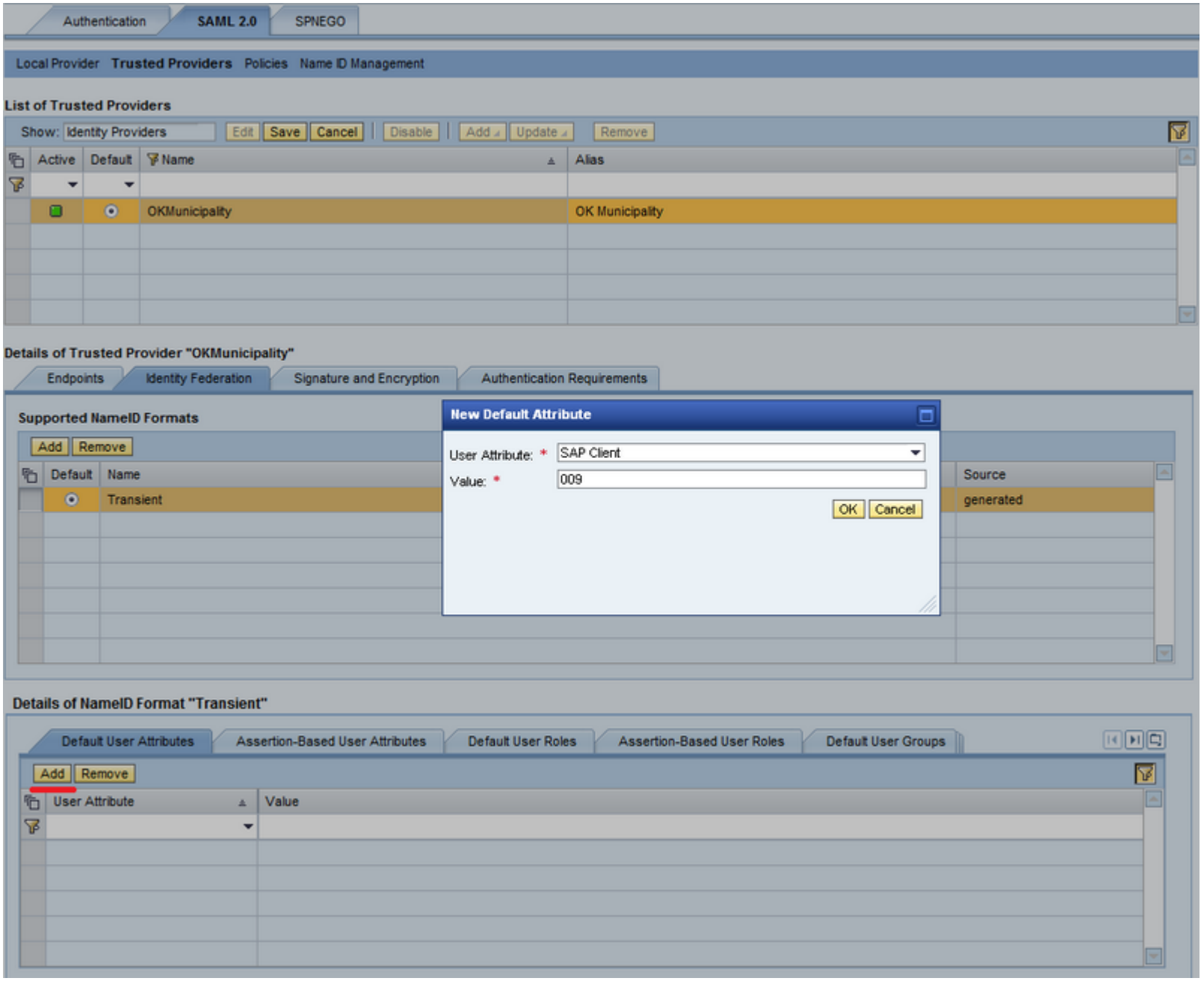
The following steps describe how to configure “Transient” name ID format, default user attributes and assertion-based user attributes.

1. Select the identity provider and click “Edit” pushbutton. Go to “Identity Federation” tab. Click “Add” pushbutton of the “Supported NameID Formats” table. Choose “Transient” format and click “OK”.



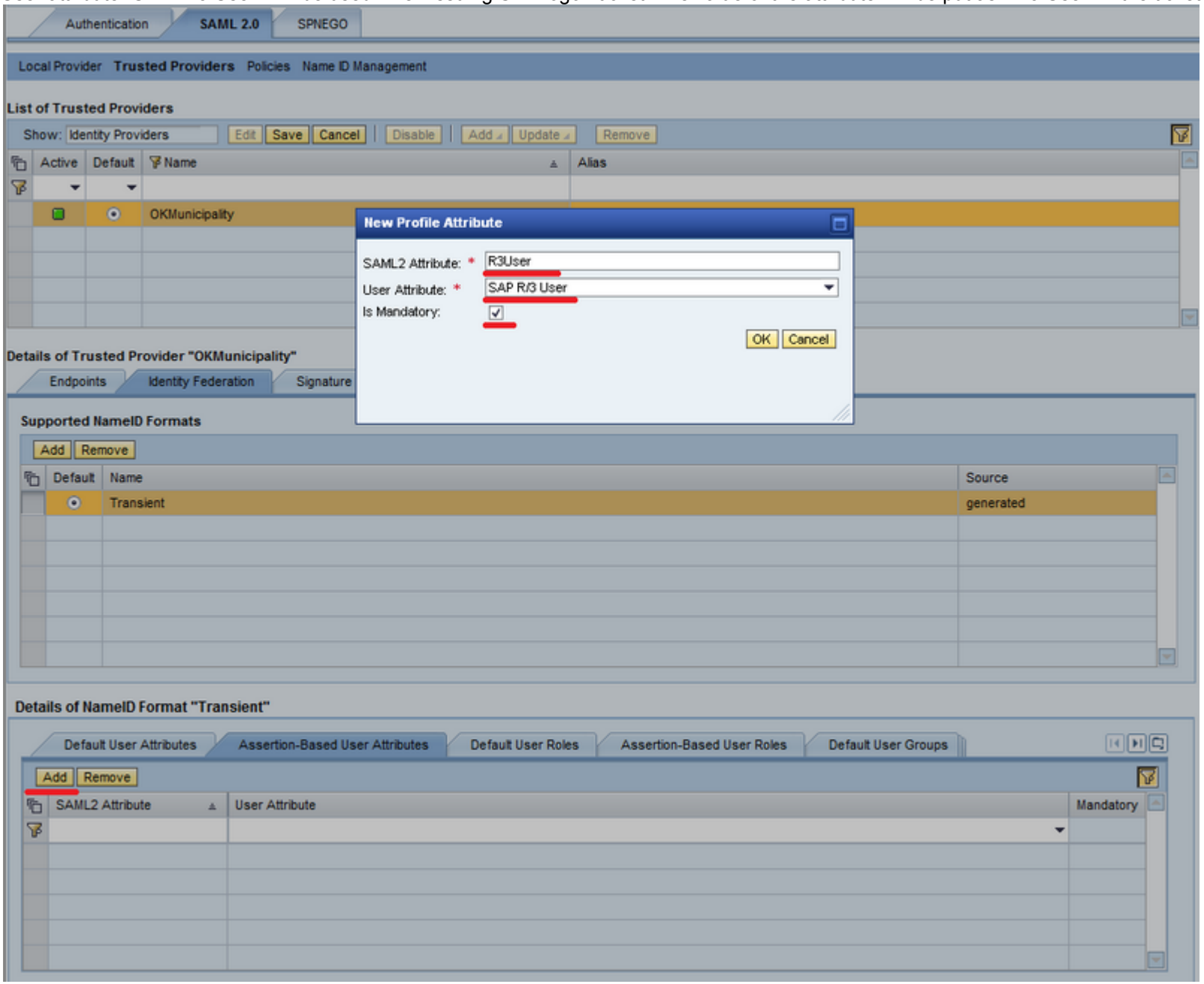
More information regarding transient name ID format can be found at help.sap.com.
For users coming from different identity providers, SAP logon ticket that will be issued needs to contain different SAP client value. For example, for users coming from company A, SAP logon tickets that are issued need to contain SAP client value “009”. SAP client “009” is the corresponding application client that company A uses on the ABAP system. For company B, the application client will have a different value.
We can achieve this by configuring default user attributes. They are stored at trusted identity provider level for transient name ID format and can be different for each trusted identity provider. Default user attributes are attributes whose values are assigned to each user coming from the configured identity provider.

2. Go to “Default User Attributes” tab and click “Add” pushbutton. Choose “SAP Client” user attribute from the drop-down. Drop-down list contains predefined user attributes and also attributes created by user.



3. Go to “Assertion-Based User Attributes” tab. Here we will configure how to interpret SAML 2.0 attributes from the assertion. In our case, we expect that identity provider knows what the account of the user in the ABAP system is and it sends it as SAML 2.0 attribute called “R3User” in the assertion.
   Click “Add” pushbutton and enter “R3User” as SAML2 attribute. Choose “SAP R/3 User” for user attribute and mark it as mandatory. Having done this, we have configured that we require that identity provider sends SAML2 attribute named “R3User” which will contain the username for access to the ABAP system. SAML 2.0 attribute “R3User” will be mapped to user attribute “SAP R/3 User”.

User attribute “SAP R/3 User” will be used when issuing SAP logon ticket. The value of the attribute will be put as “R/3 User” in the ticket.



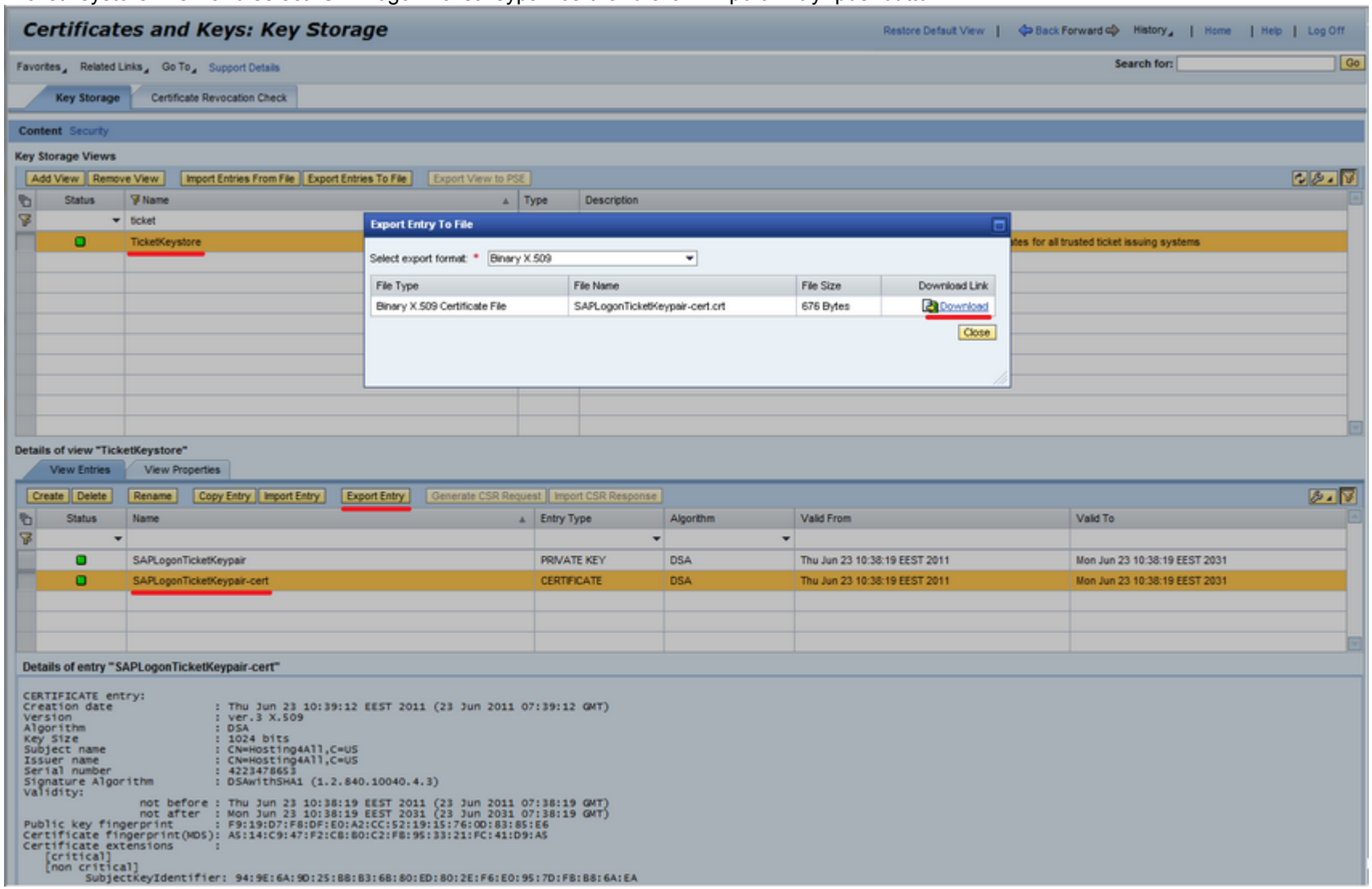
Important
In order to issue SAP logon tickets with necessary information, some additional configuration is needed. UME property **user.usermapping.refsys.mapping.type** should have value “attribute” as follows: **“ume.usermapping.refsys.mapping.type=attribute”**. Steps how

to configure the property are described at help.sap.com

Configuring ABAP System to Trust SAML 2.0 Service Provider

Video tutorial with the steps: Exporting the SAP Logon Ticket
With the following steps we will configure ABAP system to trust SAP logon tickets issued by SAML 2.0 service provider.

1. To export SAP Logon ticket certificate, open http(s)://<java server host>:<port>/nwa -> Configuration -> Security -> Certificates and Keys. Search for “TicketKeystore” view and select “SAPLogonTicketKeypair-cert” and click “Export Entry” pushbutton.



Java system on which SAML 2.0 service provider is running will issue SAP Logon tickets which contain system ID of the issuing system, client of the issuing system and logon ID of the user (logon ID used to access the ABAP system).
2. Login to the ABAP system using SAP Logon on application client which will receive SAP logon tickets(application client is "009" in our scenario). Start transaction “STRUSTSSO2”. Use the transaction to import the previously exported SAPLogonTicketKeypair certificate and adjust the ACL list. More information regarding SAP logon tickets configuration can be found at help.sap.com . Information on how to use transaction "STRUST" can be found at Using Transaction STRUSTSSO2 in SAP System >= 4.6C .

Configuring an Application to Require SAML 2.0 Authentication

With all the steps above we have configured:

- SAML 2.0 service provider of “Hosting4All”
- SAML 2.0 trust between service provider of “Hosting4All” and identity provider
- Service provider of “Hosting4All” to issue SAP logon tickets
- Legacy ABAP system to accept the SAP logon tickets issued by the SAML 2.0 service provider

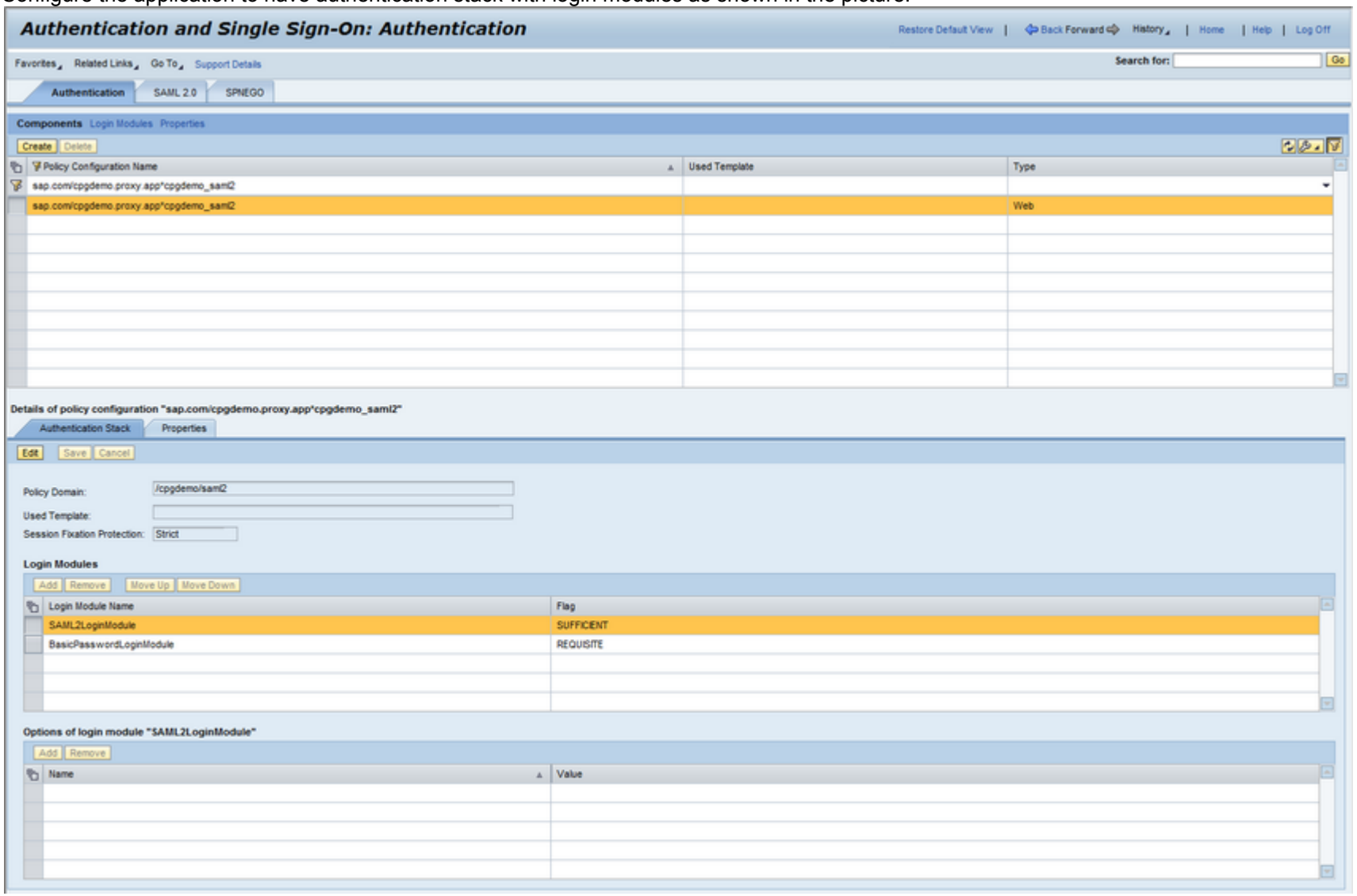
However, we still need a way to trigger SAML 2.0 authentication from the ABAP system, perform SAML 2.0 authentication and return back to the originally accessed ABAP application. For this purpose, we will use one custom Java application that will trigger SAML 2.0 authentication and redirect back to ABAP application. This application will be referred as “proxy” application.

Before the single sign-on solution is implemented, all users coming from companies A, B and Z, used to login with username and password directly on the ABAP system. In order to preserve the current entry point of the scenario, we will also modify ABAP system logon screen to have a link pointing to the proxy application. Another possibility is that end-users are given the link pointing directly to the proxy application.

Here are the steps how to achieve this:

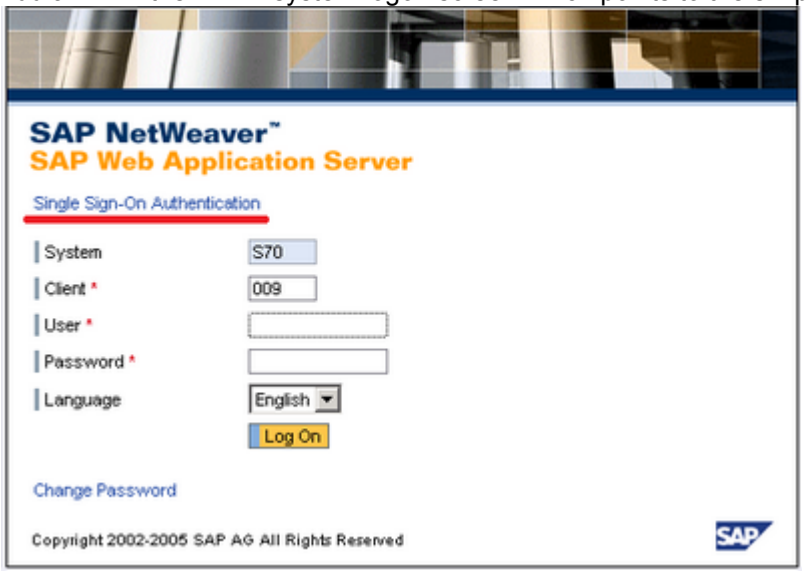
1. Create simple application which will act as a proxy between the ABAP system and identity provider. This application will be deployed on “Hosting4All” service provider system. You can find a sample application and information how to use it in SAP Note 2434765 .
2. Configure the simple application to require SAML 2.0 authentication. To do this follow the steps:
    a. Open http(s)://<java server host of “Hosting4All”>:<port>/nwa -> Configuration -> Authentication and Single Sign-On
    b. Search for the following policy configuration name: “sap.com/cpgdemo.proxy.app*cpgdemo_saml2”

c. Configure the application to have authentication stack with login modules as shown in the picture:



So we have configured that application sap.com/cpgdemo.proxy.app*cpgdemo_saml2 will have SAML 2.0 authentication. More information on protecting resources with SAML 2.0 can be found at help.sap.com

3. Add a link in the ABAP system logon screen which points to the simple application



Testing the Scenario

Let us explain what happens when end-user wants to use the single sign-on feature.

1. Users from company A access an application on the ABAP system and as usual they see the logon screen. In addition, they also see a link which points to the proxy application – for example “Single Sign-On Authentication”.
2. Users click “Single Sign-On Authentication” link and they are redirected to the proxy application hosted on the service provider system of “Hosting4All”.
3. As they do not have a session yet, they are redirected to the identity provider of company A for authentication.
4. After authenticating at the identity provider, SAML 2.0 response is sent to proxy application which evaluates it, authenticates the user, creates SAP logon ticket and redirects back to the originally accessed application on the ABAP system. ABAP system evaluates the SAP logon ticket and authenticates the user. User has access to the application.
   Video with the steps: Using Single Sign-On

Important Features Used in the Scenario

- NetWeaver AS Java 7.2/7.3 can be a broker between SAML 2.0 and SAP SSO2, e.g. to accept SAML 2.0 Assertions and to issue SAP logon tickets.
- By using SAML 2.0, NetWeaver AS Java 7.2/7.3 can work with temporary in-memory users and there is no need of user provisioning and maintenance.

saml2

43 Comments

Former Member

Hi

The link to the Sample Application has expired.

Can you update the link and/or let us know where we get a copy of the application ?

Thanks in advance

Desislava Petkova

Hi Minesh,

The link to sample application is updated. Please do let us know if you have questions or comments regarding the scenario setup.

Regards,

Desislava

Mo Ajmal

Hi Desislava,

I attempted to download the sample application and instructions but it seems to be unavailable.

Would it be possible to load the attachment again.

Regards,

Mo

Desislava Petkova

Hi Mo,

Please check if your browser has not cached the page somehow. The sample application should be available. Here is again the link sample application

Regards,

Desislava

Former Member

Hi Desislava

Many thanks for updating the link, we now have the file.

I don't know if this is the best place to discuss this, but the scenario we are working in is trying to get SAML SSO from an 3rd Party Portal to WEBGUI on the Abap Stack.

We've configured the NW 7.0 java Stack to accept SAML SSO, and now looking to see if we can have a Java Application that will redirect to WEBGUI, invoking normal SAPLogon Ticket SSO.

We were hoping this wiki and your sample application would help.

Do you have any views on this or can you offer any guidance ?

Are we on the right track ?

Thanks for any advice in advance.

Min

Kristian Lehment

Hi Min,

this kind of question should rather be asked in the discussion forum on SCN in the space for "SAP NetWeaver Single Sign-On".

Please repost your question here:

http://scn.sap.com/community/netweaver-sso/content

Thanks a lot
Kristian

Unknown User (q6gbx05)

Hi Desislava,

I attempted to download the sample application and instructions but it seems to be unavailable.

Would it be possible to load the attachment again.

Regards,

Anup

Desislava Petkova

Hello Anup,

The link is updated.

Regards,
Desislava

Unknown User (104licnjv)

Hi Desislava,

the link to the test-application has expired.

Regards,

Fabian

Former Member

Hi Desislava,

The link to the sample application expired 😞

Can you update the link and/or let us know where we get a copy of the application ?

Thanks for this wiki

Former Member

Hello Cesar,

The link has been updated.

Best regards

Angel

Former Member

Hello Angel,

Thanks, I will try to deploy the app with the NWDS.

Cesar,

Dheerendra Toutam

Hello Angel,

Thanks for the detailed blog, its very helpful. The link to the sample application has expired can you please update it.
Additionally, can you suggest how to "Add a link in the ABAP system logon screen which points to the sample application"

Thanks in advance.

Dhee

Former Member

Hi Dhee,

The link for the sample application was updated.

Regarding the link ot the ABAP logon screen there are two options:

1. For SAP_BASIS releases 7.30 and higher: Open SICF transaction, find your node/alias, open it, click the button "Change" (the first one on the toolbar). Then go to tab "Error pages", tab "Logon Errors" below it and click the radio button "System Logon" and the button "Configuration" next to it. The dialog "System Logon Configuration" appears. Now click the button "Adjust Links and Images". In the section "Configurable Links in Header Area" you can define links which will appear in the header of the logon page as on the screenshot above.

2. For releases lower than 7.30 you can implement your own handler which meets your requirements. To do this, implement a separate class that overwrites certain methods of the class CL_ICF_SYSTEM_LOGIN, especially the method HTM_LOGIN. Example of such a class is CL_ICF_EXAMPLE01_LOGIN which shows a custom logon screen. You have to configure your handler in SICF. Just like in point 1. open the dialog "System Logon Configuration". Then click the button "Define Service-Specific Settings" and in the section "Logon Layout and Procedure" click the radio button "Custom Implementation" and specify the name of your custom class which extends CL_ICF_SYSTEM_LOGIN.

I hope this will help you for the moment. I'm currently in contact with ICF developers about this custom logon screens and when I find the optimal solutions for every release I'll update the section in the wiki above.

Best regards

Angel

Former Member

Hello

I Install SAP NetWeaver AS Java 7.4 SR1 Java system facing issue with **"Uploading Metadata File"** Error mention below

Metadata contains trusted provider which is not an identity provider

Please suggest if any configuration is require**?**

Tejas

Former Member

Hello,

If you are trying to setup a trusted Identity Provider on the Service Provider side than your metadata most likely doesn't contain an Identity Provider.

If you're sure that the metadata is OK open a customer ticket in BC-JAS-SEC and attach the metadata.

Best regards

Angel

Former Member

Hello Angel

what is SAML 2.0 requirement With Domain or Without Domain system?

Thanks

Tejas

Former Member

Hi Tejas,

Where did you find this requirement?

Best regards

Angel

Former Member

Hello Angel

I am Keen too know about this so I approached you. Do you have any idea about it

SAML 2.0 working only Domain system ?

Thanks

Tejas

Former Member

Hi Tejas,

In principal SAML 2.0 is a cross-domain SSO mechanism. This wiki describes a way to provide SSO for users authenticated with SAML 2.0 to legacy ABAP systems(which don't support SAML 2.0) with SAP Logon tickets.

Best regards

Angel

Vamsi Krishna Srikanti

Nice document, thank you.

Former Member

Can you please eloberate following?

As metadata is signed by a certificate that is self-signed, in order to verify it we need to select a copy of the certificate used to sign the metadata ?

I am also getting the same error.

How to get the copy of the certificate used to sign the metadata.

Regards

Former Member

Hi,

ABAP SP doesn't evaluate certificates included in the assertion. You need to have the certificate in advance and import in ABAP SP SAML 2.0 configuration.

How to obtain it is a question of the IdP implementation. In most of the cases IdPs allow to download their metadata(which includes the certificates) from a link. Then you can import this metadata in ABAP SP to establish the trust. The certificate will be automatically imported.

Regards

Angel

Former Member

Thanks Angel!!

I am done with this but currently i am facing other issue as follows:

I setup sap authenticator for fiori and when i click fiori apps its asking user name and password(But it should not)?

Do we need to use ABAP UME for java systems where we installed/configured idp?

Regards

Syed

Former Member

Hi Syed,

Basic authentication pop-up means that SAML 2.0 authentication has failed. Start ABAP SAML 2.0 traces, reproduce the problem and check the logs for more details.

If you can't find the reason for the failing authentication (check the following wiki: Common Problems When Configuring SAML 2.0 for AS ABAP and search SAP notes first) open a ticket on BC-SEC-LGN-SML component.

What should be the user source on the java system with IdP depends on your scenario - it might be the ABAP UME, but it's not necessary. In SAML 2.0 world the users on SP and IdP sides are usually different and SAML's main task is to do the mapping between them.

Best regards

Angel

Former Member

Thank, yes i tried abap saml traces but no error found there.

I am confused here.

Former Member

Only thing i can see is under user tab/row is <no user>? I think that should show user name but its not showing for me.

Client	Server	Work Process	Time	Severity	User	Message

Former Member

Hi Syed,

Unfortunately this wiki is not for issue tracking, please open a ticket on BC-SEC-LGN-SML component.

Best regards

Angel

Narayanan K B

Hi

I have deployed he sample application in my Service Provider Server but not able to find URL of this application. I am not a developer so have very little knowledge of Application development.

Can someone help me to find http URL of this sample application.

Regards

Ghanshyam Yadava

Former Member

Hi,

The URL is:

<your java server host and port>/cpgdemo/saml2/redirect

Best regards Angel

Narayanan K B

Hi

Dear Angel Penkov

Thanks for your support. I could call application directly.but now i am facing another issue. Grateful if you can help me

I have made setup with 3 systems. ES1(SAML SP) ED1(SAML IdP) and one abap system running FIORI. i have deployed application in ES1 and i am calling URL directly.The URL is executed successfully and redirected to ED1(IdP) for authentication but after successfull authentication it is again redirected to ES1 instead of ABAP system and again authentication is challenged in ES1. even after providing user id and password of ES1, request is not directed to abap system the screen becomes blank.

not sure if am missing anything or more settings are required.

request for help

Regards

Ghanshyam Yadava

Former Member

Hello,

Please check that you have performed all steps from section "Configuring an Application to Require SAML 2.0 Authentication". If after this it's not working again this can be checked in an SAP ticket in BC-JAS-SEC component.

Best regards

Angel

Former Member

Hi ,

Can someone help , I have deployed demo app but its not accessible , Is there anything to do to activate this demo app in portal.

http://servername:50100/cpgdemo/saml2/redirect

Evgeniy Serebrennikov

Hello.

We have successfully installed SAML according to instructions.

On server provider side next errors:

#2.#2016 05 19 14:44:16:191#+0300#Error#com.sap.security.saml2.sp.UserMappingService#

com.sap.ASJ.saml20_sp.000068#BC-JAS-SEC#sap.com/saml2_sp#C000053DEDA602700000000010000021CB#9928550000000004#sap.com/cpgdemo.proxy.app#com.sap.security.saml2.sp.UserMappingService
#Guest#0##BCD314AF1DB611E6ADE3000000977F66#bcd314af1db611e6ade3000000977f66#bcd314af1db611e6ade3000000977f66#0#Thread[HTTP Worker [@1894622118],5,Dedicated_Application_Thread]#Plain##
Service Provider could not update user account attributes for Subject Name ID [NID-T-xL5wv/dNaPCZ/dj7jzBvNffWu80=] received from Identity Provider [zmobilepi] because mandatory profile attribute [SAML2 attribute name: R3User, is mandatory: true, UME attribute alias: SAP R/3 User, UME attribute name: null, UME attribute namespace: null
cfg path: default/trusted_providers/trusted_idps/0/identity_federations/6/profile_attributes/0] is not found in SAML2Assertion attributes [Attributes].#

Could you please comment it. Look like IP does not send nessary attributes. Thank you.

Also we have created incident in SAP 135186 / 2016, but nobody has been aswered. 135186 / 2016

Desislava Petkova

Hello Evgeniy,

Yes, it seems that IdP is not sending the attribute "R3User" as it is not found in the SAML assertion. Have you configured IdP to send this attribute in SAML Assertion?

What IdP are you using?

Best regards,

Desislava

Evgeniy Serebrennikov

Hello.

I am happy to see your responce.

"Have you configured IdP to send this attribute in SAML Assertion?" How can we do that?

"What IdP are you using?" SAP Netweaver 7.5 Java system

We have installed IdP on SAP Netweaver 7.5 Java system as in instruction guide. I could not find any configuration steps how to set IdP to send attribute "R3User" to Service Provider.

Desislava Petkova

Hi,

Please check the following link http://help.sap.com/saphelp_nwsso20/helpdata/en/0a/785879e2ec4db3b6e8a4fea4fef7f5/content.htm?frameset=/en/64/38385003ce4f2d88602fbf0de78f2f/frameset.htm&current_toc=/en/64/38385003ce4f2d88602fbf0de78f2f/plain.htm&node_id=33.

Do your scenario require exactly such SAML attribute?

Regards,

Desislava

Evgeniy Serebrennikov

Hello.

Thank you for your reply.

On the IdP side I have added some attributes for trusted providers of my Service Provider.

It is work when I use Default Assertion Attributes, but in this case I have to enter concret username.

It is not work when I use User-Based Assertion Attributes. (SAP R\3 User). I don`t understand why, the error as the as I mentioned.

And we have one more problem. When I am watching session in Session monitor of SP, the username of user which have made login by idP, has name such a "USER NAME = NID-T-FQCZ1ChHw6VuVql0DruJ0uGOeqI=". I think that usermapping does`t work. It is problem, because we can not do central logout for concret user.

From documentation I found:

"You want users to log off from all systems, where they have a session.

SAML enables Single Log-Out (SLO). When a user logs off from a service provider, the service provider notifies the identity provider, which in turn notifies all other service providers, where the user has a session." How can we do that? Is it possible to do with example of this arcticle?

Desislava Petkova

Hi Evgeniy,

I suggest that you create a discussion in NetWeaver SSO community http://scn.sap.com/community/sso/content and we can continue discussing there.

Regards,

Desislava

Armaghan Shahzad

Hi Desislava,

The link to the sample application expired 😞

Can you update the link and/or let us know where we get a copy of the application ?

Regards

Desislava Petkova

Hello,

I updated the link to the application.

Regards,

Desislava

Ashutosh Tiwari

Hi Desislava,

The link to application has expired.

can help update the link.

Thanks !!

Desislava Petkova

Hi Mayank Garg,

Did you check the attachments in SAP Note 2434765? Application is attached to the note.

Best regards,

Desislava