otherside at work

for happy professionals

SINGLE SIGN ON IMPLEMENTATION

SAML2

AUTHOR Axel de Mol

VERSION 3.0

STATUS Definitive

DATE November 15th, 2021

CLASSIFICATION Public

powered by fair priced technology

CHANGE HISTORY

Version	Date	Status	Change	Author
1.0	09-07-2015	Definitive	Basic design	Stef Roskam
1.1	24-01-2017	Definitive	Addition extra information	Stef Roskam
2.0	31-01-2019	Definitive	Implementation new corporate identity, new conditions	Stef Roskam
3.0	15-11-2021	Definitive	English Translation	Axel de Mol

TABLE OF CONTENTS

1 INTRODUCTION

This document outlines the possibilities for connecting the Xpert Suite with an external Identity Provider using the SAML 2 protocol, in order to realise Single Sign On between the customer's systems and the Xpert Suite.

2 CONNECTED SYSTEMS

The Xpert Suite can be connected to the following Identity Providers. Where known, any particularities regarding the implementation are described below.

- Microsoft ADFS (On Premise)
- Microsoft Azure AD - Because the metadata is not automatically updated, a Tennant-Specific Metadata Endpoint is advised. This allows better verification of rollover of certificates.
- Google IDP - Adding the Xpert Suite as a Service Provider will make the application available users as a button. However, using this button executes an IDP-Initiated Sign On, which we do not support. Instead, calling our application will execute a successful SP-initiated Sign On using Google IDP.
- Open-A-Select
- Ping Identity
- SurfConext

3 PRECONDITIONS AND POINTS OF ATTENTION

- The authentication requests must be initiated via Xpert Suite (SP-initiated). The Xpert Suite does not support IDP-initiated Sign On.
- The Xpert Suite does not support automatic metadata updates. Changing certificates on the IDP side must be communicated well ahead of time. Certificates can be added prior to the certificate exchange. The customer remains responsible for delivering the new certificates in a timely manner.
- It is not necessary to make the IDP publicly accessible because of the use of browser redirects on the client-side browser.
- Authentication response messages must be signed, and we do not support encryption of response messages.
- Authentication requests are signed using self-signed certificates. The Identity Provider must be able accept these certificates.
- If a customer also uses an interface which creates users automatically in the Xpert Suite, it is possible to enable these users to login directly via SSO as well. As a precondition, the SAML authentication response must then contain a value for Subject/NameID or claim matching the value(s) provided by the interface. That value can then be used to create automatic mapping.

- Authentication requests send a HTTP-REDIRECT (GET) to the Identity Provider via the clients' browser.
- Authentication responses expect a HTTP-POST from the Identity Provider via the clients' browser.

4 IMPLEMENTATION STEPS

1. Please consider and answer the below:
    - Which Identity Provider will be used?
    - Can you deliver the metadata directly?
    - Choice of domain and subdomain, for every connected IDP we use a different subdomain for acceptance and production environments:
    - [subdomain].xpertsuite.nl
    - [subdomain].accxpertsuite.nl
        - The .app suffix is also possible instead of the .nl suffix.
    - Do you have an acceptance IDP which has to be connected to an acceptance Xpert Suite environment?
    - What will you use as the Net-ID (unique ID for the user)?
2. An intake is planned where we will discuss the following actions (see below).
    - After receiving the metadata, we will configure the system on our side and provide a link containing our metadata. With that metadata you can configure your IDP.
    - Testing the technical connection: We will provide a link you have to follow from your IDP environment. If all is in order, you will get a response that the user is not registered. This response means the connection is working correctly. The response message is checked and processed correctly. If you get an error, it can have the following causes:
        - Subject/NameID is not delivered in the response message. E.g., the IDP not accepting the Self Signed Certificates.
        - The signing can't be checked.
3. We convert an existing user to a Single Sign On user and test the SSO login.
4. Converting existing users:
    - We will agree a time for converting the rest of the users from username/password to Single Sign On.
    - For a large userbase: a conversion can be set up to convert the users in one go.
    - For a small userbase: The Xpert Suite administrators can convert them manually using the User Administration module of the Xpert Suite.

- Adjust the interface if necessary, so new users can log in automatically with Single Sign On.

5 MESSAGE EXAMPLES

5.1 METADATA XPERT SUITE

```
<?xml version="1.0" encoding="utf-8"?>
<q1:EntityDescriptor entityID="testurl.xpertsuite.nl" validUntil="2014-10-
09T12:23:01.7077870Z" ID="id0e0f19fc6aaa45cda3affa92e413438a"
    xmlns:q1="urn:oasis:names:tc:SAML:2.0:metadata">
    <q1:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
AuthnRequestsSigned="true" WantAssertionsSigned="true">
        <q1:KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
                    <X509Certificate>[Custom certificate]</X509Certificate>
                </X509Data>
            </KeyInfo>
        </q1:KeyDescriptor>
        <q1:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://testurl.xpertsuite.nl/account/logoff"
ResponseLocation="https://testurl.xpertsuite.nl/account/logoff" />
        <q1:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://testurl.xpertsuite.nl/account/logoff"
ResponseLocation="https://testurl.xpertsuite.nl/account/logoff" />
        <q1:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://testurl.xpertsuite.nl/account/singlesignon" index="0"
isDefault="true" />
        <q1:AttributeConsumingService index="0" isDefault="true">
            <q1:ServiceName xml:lang="da">SP</q1:ServiceName>
            <q1:RequestedAttribute Name="urn:FirstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
            <q1:RequestedAttribute Name="urn:LastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
            <q1:RequestedAttribute Name="urn:Age"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" />
        </q1:AttributeConsumingService>
    </q1:SPSSODescriptor>
    <q1:ContactPerson contactType="administrative">
        <q1:Company>Empirion BV</q1:Company>
        <q1:GivenName>Support</q1:GivenName>
        <q1:SurName>Empirion</q1:SurName>
        <q1:EmailAddress>info@empirion.nl</q1:EmailAddress>
        <q1:TelephoneNumber>073-6159950</q1:TelephoneNumber>
    </q1:ContactPerson>
```

```
</q1:EntityDescriptor>
```

5.2 AUTHENTICATION REQUEST XPERT SUITE

```
<?xml version="1.0"?>
<q1:AuthnRequest ID="id1bfd6a2df1b8467394ffa50f86566750" Version="2.0" IssueInstant="2014-
10-02T12:39:14.5839382Z" Destination="https://sso-provider.klant.local/adfs/ls/"
ForceAuthn="true" IsPassive="false"
    xmlns:q1="urn:oasis:names:tc:SAML:2.0:protocol">
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">testurl.xpertsuite.nl</Issuer>
    <q1:NameIDPolicy AllowCreate="true" />
    <Conditions xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <AudienceRestriction>
            <Audience>testurl.xpertsuite.nl</Audience>
        </AudienceRestriction>
    </Conditions>
</q1:AuthnRequest>
```