SAML IDP SINGLE SIGN-ON API

October 2020

Xpressdocs Partners, Ltd. 1301 NE Loop 820, Fort Worth, TX 76137, USA

+1 817.547.9743 | www.xpressdocs.com

Contents

1 Introduction

SAML is an XML-based open standard data format for exchanging authentication and authorization data between parties. SAML allows for web browser single sign-on and thus the sharing of services between companies while using only the user's company authentication servers. This means a client can use the services of Xpressdocs through their browser without having to remember another login or password. This technical document describes the details of the protocol required to utilize the services of the SAML Single sign-on System.

1.1 Security

Xpressdocs SAML Single sign-on requires the Clients' Identity Provider SSO Link ID to allow access to the Xpressdocs platform. The Xpressdocs user account's link id should match with Identity provider's local user ID.

1.2 Acronyms and Definitions

This section provides definitions for all acronyms and terms introduced in this document.

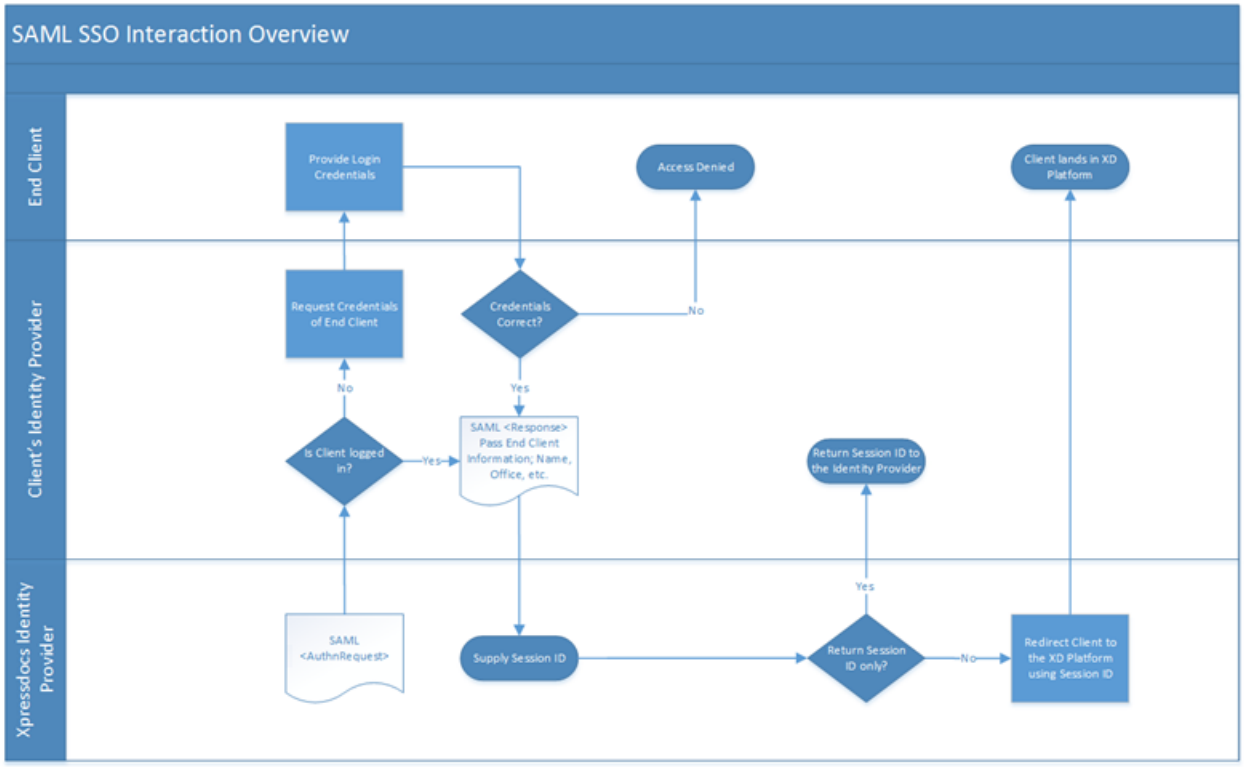
Acronym	Definition
SAML	Security Assertion Markup language
SP	Service Provider: Business partner application looking to integrate.

1.3 Assumptions

1. All SAML timestamp values must be compliant to W3C XML schema data type specification and must be expressed in UTC with no time zone component
2. All SAML identifiers such as assertions, request and response ID's should ensure that identifier is unique.
3. Encoding the URL for RelayState is up to the business partner's (service provider) implementation.
4. The business partner (service provider) servers and Identity Provider SSO server's time will be in sync to use the response timestamp for validation. The time should be synced against the time-b.nist.gov NTP server

2 SAML Integration Flow

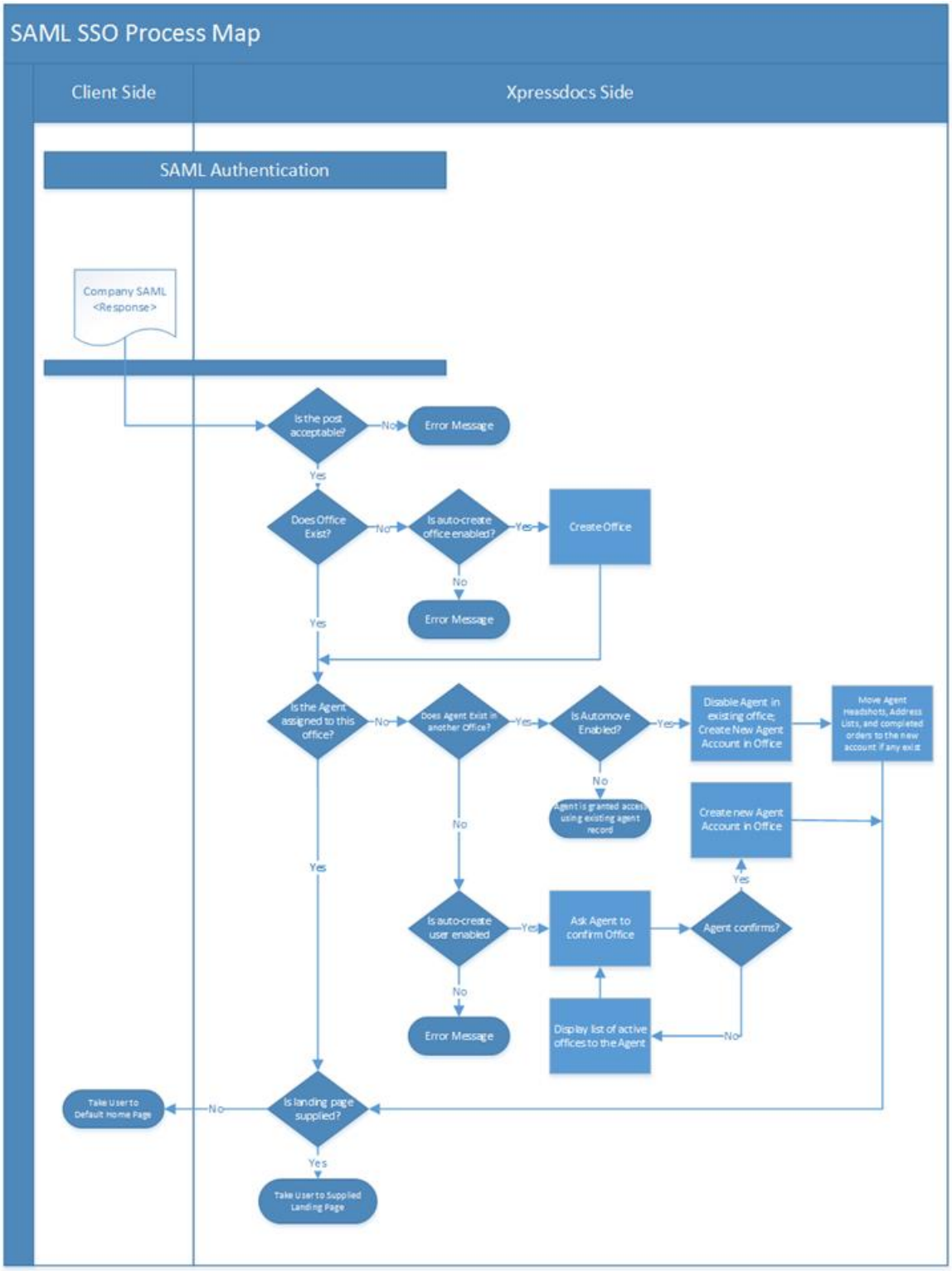
2.1 Detailed SAML Interaction Overview



2.2 Detail SAML Interaction Steps

1) Client's Identity Provider provides a SAML response (See 3.1.1 Sample SAML Response XML for an example) to Xpressdocs passing on the Client's information; Name, Office, etc.
2) Xpressdocs generates an authenticated session
3) Xpressdocs redirects the Client's browser to the Xpressdocs Platform with their Session ID

2.3 SAML SSO Process Map



2.4 SAML SSO Process Map Steps

1) Client's Identity Store sends a SAML response
2) Xpressdocs validates the response and compares it against the data we currently have on the client
   a) If the post is corrupt or otherwise unacceptable an error message is displayed
3) The system then checks if the office the Client is a member of exists
   a) If the office does not exist the system will attempt to auto-create the office.
      i) If auto-create office is disabled an error will be displayed, "*Attempt to create Office account or Login was not successful. Contact your account manager at Xpressdocs for assistance. 1.866.977.3627*"
      ii) If auto-create office is enabled it will create the office
4) The system checks to see if the Client shows as a member of that office in the Xpressdocs system.
   a) If the Client isn't assigned to the office the system checks to see if the Client's account exists.
      i) If the Client's account doesn't exist the system will attempt to auto-create the Client's account.
         (1) If auto-create user is disabled an error will be displayed, "*Attempt to create User account or Login was not successful. Contact your account manager at Xpressdocs for assistance. 1.866.977.3627*"
         (2) If auto-create user is enabled, it will create the Client's account.
   b) If the agent exists the Xpressdocs system attempts to move the user to the office.
      i) If auto-move is disabled, then the Client is left in their existing office and granted access to the Xpressdocs system.
      ii) If auto-move is enabled, the Client is added to the office along with their headshots, address lists, and completed orders.
5) Xpressdocs checks to see if a Landing Page URL was supplied with the Login Request
   a) If not, the Client is taken to the default home page for the customer
   b) If so, the Client is taken to the specified landing page

3

3 Identity provider sends SAML Response

3.1 SAML Response

A SAML response will be sent to the service provider. SAMLResponse is a form post parameter. The important elements/attributes contained in the SAMLResponse are as follows

Fields marked with an asterisk (*) are required if the auto-update user or office preference is set to YES

Element Name	Description	Req'd
InResponseTo	This will be set to the authn request Id that was received by the Identity provider. This can be used for validating the response	Y
Destination	This is where the SAML response is sent (Assertion Page URL)	Y
StatusCode	Status code (Success or Failure)	Y
StatusMessage	Status message	Y
NotBefore1	SAML response is valid from this time.	N
NotOnOrAfter2	SAML response is valid until this time.	N
Assertion Attributes : UserID	User Id: Unique Identifier of the user record, used for identifying the user	Y
Assertion Attributes : UserName	User Name associated with User Id	N
Assertion Attributes : EmailAddress	Email Address of the user	Y
Assertion Attributes : FirstName*	First name of the associated user	For New
Assertion Attributes : LastName*	Last Name of the associated user	For New
Assertion Attributes : OfficeId	Unique Identifier of the office record, used for identifying the office in Identity Provider System.	Y
Assertion Attributes : Role	Role of the User: Agent / Office Admin / Company Admin	Y
Assertion Attributes : OfficeName*	Office name	For New
Assertion Attributes : OfficeLegalName	Office legal name if different than office name	N
Assertion Attributes : OfficeAddress1*	Address1 field	For New
Assertion Attributes : OfficeAddress2	Address2 field	N
Assertion Attributes : OfficeCity*	City	For New

[1] The Server time should be synced against time-b.nist.gov NTP server.

Assertion Attributes : OfficeState*	State	For New
Assertion Attributes : OfficeZip*	Zip	For New
Assertion Attributes : OfficePhone*	Office Phone number	For New
Assertion Attributes : OfficeFax	Office fax number	N

Assertion Attributes : LandingPageURL	Page to drop user onto following a successful login:
	• (Default) Home - /index.php
	• APM Properties - /apm_pending.php
	• APM Property Marketing Program Preferences - /apm_profile.php
	• Brand Essentials/OPS – /stationery.php
	• Calendar Creation – /calendar.php
	• My Account - account/index.php
	• MyListings - /mylisting_results.php
	• New Email - /rezora_sso.php?new=1&
	• Print and Direct Mail landing page - categories.php
	  ○ Can include linking to a specific category or template
	• Seasonal page - seasonal.php
	• Social HQ landing page - /marketing_socialhq.php
	• Stat a new Order – /template.php
	  ○ Can include linking to a specific category or template
	  ○ XpressConnection landing page - xpressconnection/index.php
		N

3.1.1 Sample SAML Response XML

Note: The content in the sample SAML response, color coded (optional attributes) is generated based on the Schema defined in *SAML OASIS Documentation*.

Please refer to the *above table* for the important attribute and elements that contains the assertion values in the SAML response.

```
<samlp:Response ID="_03013930-4bd3-4ce9-8462-b3865792bffd"
InResponseTo="_5348301c-0016-476e-8b2d-117be490b50d" Version="2.0"
IssueInstant="2012-03-02T16:09:16.425Z"
Destination="http://www.example.com/ProcessSamlResponsePage.aspx"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://www.example.
com/IDProvider/</saml:Issuer>
```

```
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
/>
  <samlp:StatusMessage>Authenticated the user: Jane Doe
</samlp:StatusMessage>
  </samlp:Status>
<saml:Assertion Version="2.0" ID="_a999fd99-44f6-42a2-8033-
46393aa58789" IssueInstant="2012-03-02T16:09:16.425Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>http://www.example.com/Idprovider/</saml:Issuer>
<saml:Subject>
  <saml:NameID>Jane.Doe@domain.com</saml:NameID>
<saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <saml:SubjectConfirmationData Recipient="
http://www.example.com/ProcessSamlResponsePage.aspx"
  </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2012-03-02T15:59:16.425Z"
NotOnOrAfter="2012-03-02T16:19:16.425Z" />
<saml:AuthnStatement AuthnInstant="2012-03-02T16:09:16.425Z">
<saml:AuthnContext>
  <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pas
sword</saml:AuthnContextClassRef>
  </saml:AuthnContext>
  </saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="UserID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserID">
  <saml:AttributeValue>12345</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="UserName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserName">
  <saml:AttributeValue>Jane Doe</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="EmailAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="EmailAddress">
  <saml:AttributeValue>Jane.Doe@domain.com</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="FirstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="FirstName">
  <saml:AttributeValue>Jane </saml:AttributeValue>
  </saml:Attribute>
```

```
<saml:Attribute Name="LastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="LastName">
 <saml:AttributeValue>Doe</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeId ">
 <saml:AttributeValue>12345ABCD</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="Role"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Role">
 <saml:AttributeValue />
 </saml:Attribute>
<saml:Attribute Name="OfficeName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeName ">
 <saml:AttributeValue>Demo Branch</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeLegalName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeLegalName ">
 <saml:AttributeValue>Demo Branch</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeAddress1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeAddress1">
 <saml:AttributeValue>123 some street</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name=" OfficeAddress2"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeAddress2">
 <saml:AttributeValue>Suite 300</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeCity"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName=" OfficeCity ">
 <saml:AttributeValue>Fort Worth</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeState"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="OfficeState">
 <saml:AttributeValue>TX</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeZip"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="OfficeZip">
```

```
 <saml:AttributeValue>76137</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficePhone"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="OfficePhone">
 <saml:AttributeValue>123-432-1234</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute Name="OfficeFax"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="OfficeFax">
 <saml:AttributeValue>123-423-1234</saml:AttributeValue>
 <saml:Attribute Name="Landing_Page_URL"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="LandingPageURL">
 <saml:AttributeValue>template.php</saml:AttributeValue>
 </saml:Attribute>
 </saml:AttributeStatement>
 </saml:Assertion>
 </samlp:Response>
```

4 Service provider process SAML response

4.1 Overview

The service provider receives the SAML response and should process the SAML assertion. The following section describes the process.

4.2 Process SAML Assertion

The service provider's Assertion page is responsible for both receiving the SAML response and processing the response.
This section describes pseudo code for processing SAML response.

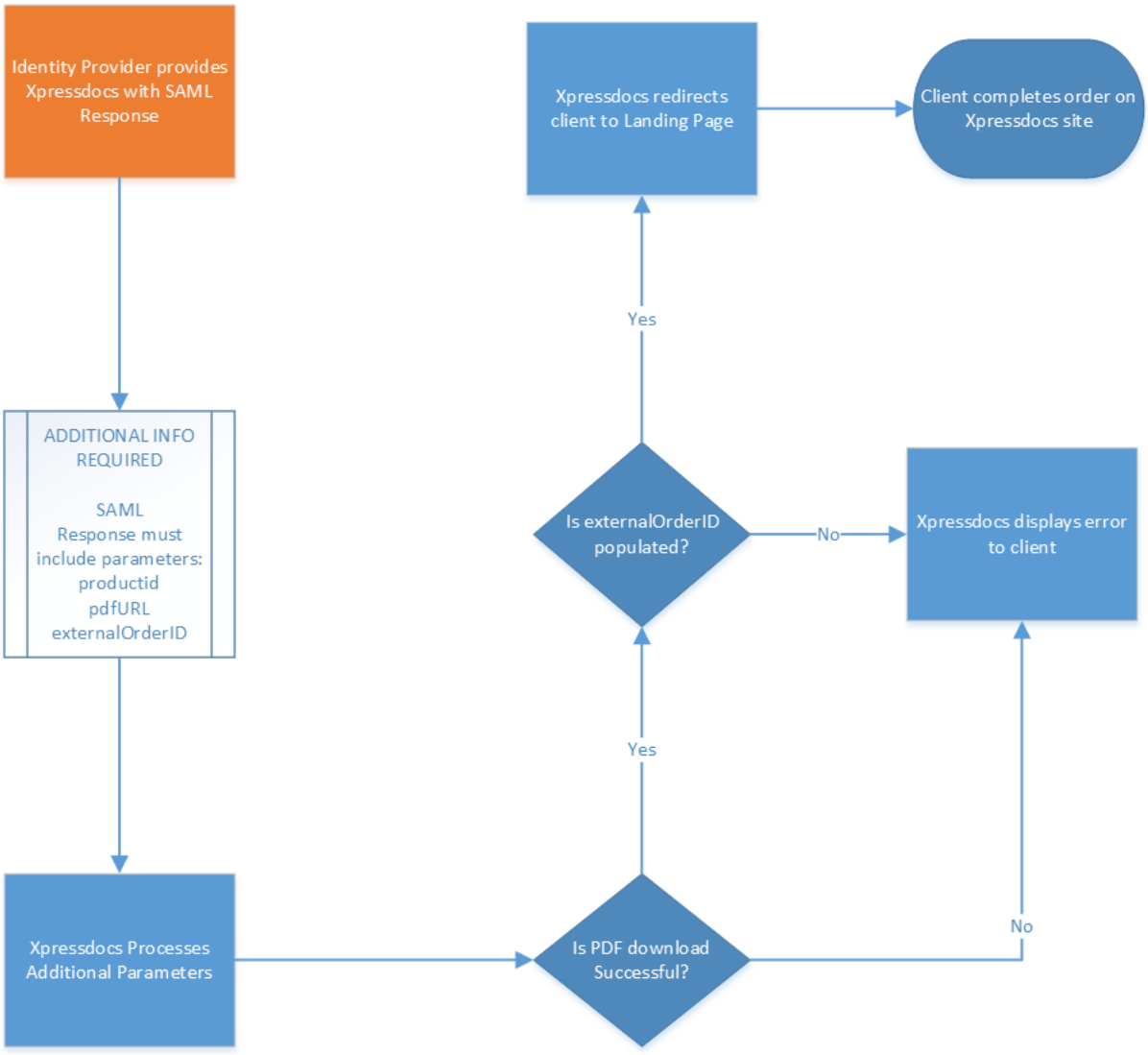
1. Receive the SAML response.
    a. Store the SAMLResponse in session.
2. Process SAML response.
    a. If the statuscode == success then it processes the assertion

Otherwise throw an exception or display custom error message.

    b. To process the assertion check for the assertion attributes.
        i. If the assertion attributes is not null then validate the attributes
        ii. Validate all the assertion attributes in the SAML response and redirect the page that the user requested which can be retrieved via the RelayState parameter.

5 Order Integration

5.1 Detailed Order Integration Overview



5.2 Overview

The Client will call Xpressdocs Order Integration by adding Order Integration parameters to a the initial SAML response sent to the link provided by Xpressdocs.

5.3 Request

The Client will input the order as additional attributes in the initial SAML response:

Field	Description	Required	Value Type
pdfUrl	Client provided location of print-ready-file	YES	String
externalOrderId	Client's unique order reference number	YES	Alphanumeric or Numeric
productid	Product code provided by Xpressdocs	YES	Alphanumeric
templatekey	Template key provided by Xpressdocs	No	Alphanumeric

```
<saml:Attribute Name="pdfUrl"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="pdfUrl">
  <saml:AttributeValue>https://sampleurl.pdf</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="externalOrderId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="externalOrderId">
  <saml:AttributeValue>123UnqiueNumber</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="productid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="productid">
  <saml:AttributeValue>SMPC</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="templatekey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="templatekey">
  <saml:AttributeValue>12345</saml:AttributeValue>
  </saml:Attribute>
```

5.4 Validation of Request

1. Xpressdocs will download the PDF at the provided **pdfUrl**.
    1. Xpressdocs will validate that the pdf url is accessible. In the event of an error, an error message will be generated to user.
2. Next, Xpressdocs will verify the **externalOrderId** is not empty.
    1. The Client must provide a unique reference identifier for each order to ensure tracking of all orders. If this value is not provided, an error message will generate to user.
3. Finally, Xpressdocs will verify that the **productid** &/or the **templatekey** were provided.
    1. The Client must provide either the templatekey that associates their template to the corresponding Xpressdocs template or the Xpressdocs productid that is associated with their template.
        1. This allows Xpressdocs to match the pdf to the appropriate product and to handle special case needs such as page orientation.
        2. If neither of these are provided an error message will generate to user.

5.5 Order Creation

Xpressdocs will create a new order and populate the known fields, including the externalOrderId as provided by the Client. Xpressdocs will redirect users into the Xpressdocs Platform. The user will then complete the order through the Xpressdocs platform order flow.

5.6 Diagnostics

Xpressdocs logs all responses received from Clients. Xpressdocs recommends that Clients do this as well. Troubleshooting issues is much easier when a clear record of what data was exchanged exists, including error messages and what happened as a result.

5.7 Tasks

Xpressdocs needs to do the following to integrate with a Client:

1. Xpressdocs must provide Clients with product IDs &/or template keys
2. Xpressdocs must support both SAML SSO and Order Integration setup with Client
3. SAML SSO integration requires validation of SAML attribute exchange
4. Upon successful testing of SAML integration, then Order Integration testing can begin
5. Xpressdocs must coordinate both SAML SSO and Order Integration testing with Clients prior to deployment

6 Links to oasis documents

http://saml.xml.org/saml-specifications