Setting up Federated Identity with LotusLive™

Version 1.0

IBM

Lotus software

Notices

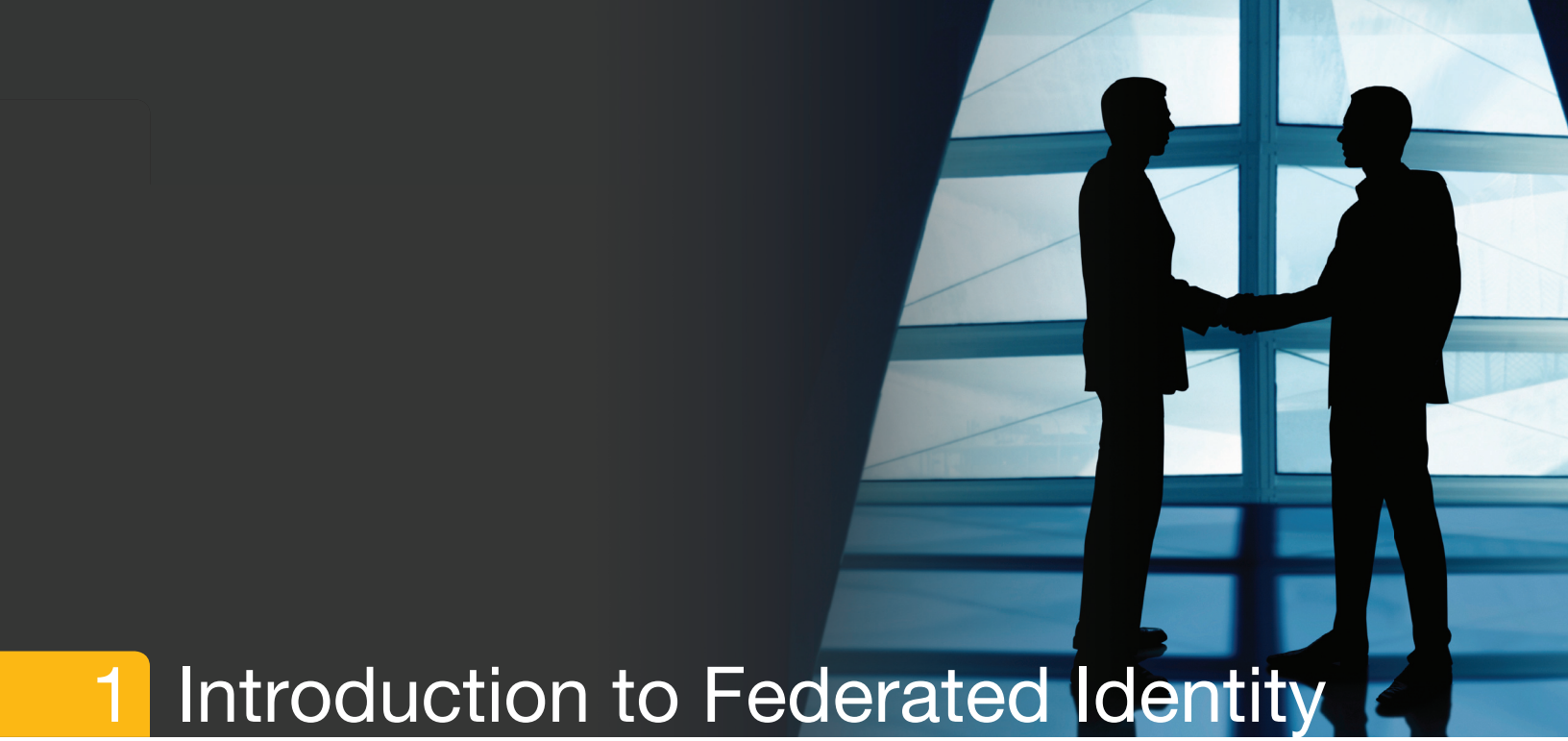
International Business Machines Corporation provides this publication “as is” without warranty of any kind, either express or implied. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore this statement may not apply to you.

This publication may contain technical inaccuracies or typographical errors. While every precaution has been taken in the preparation of this document, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/ or changes in the product(s) and/or the program(s) described in this publication at any time.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license enquiries, in writing, to the IBM Director of Commercial Relations, IBM Corporation.

The following terms, used in this publication, are trademarks or service marks of corporations in the United States or other countries:

Contents



1 Introduction to Federated Identity

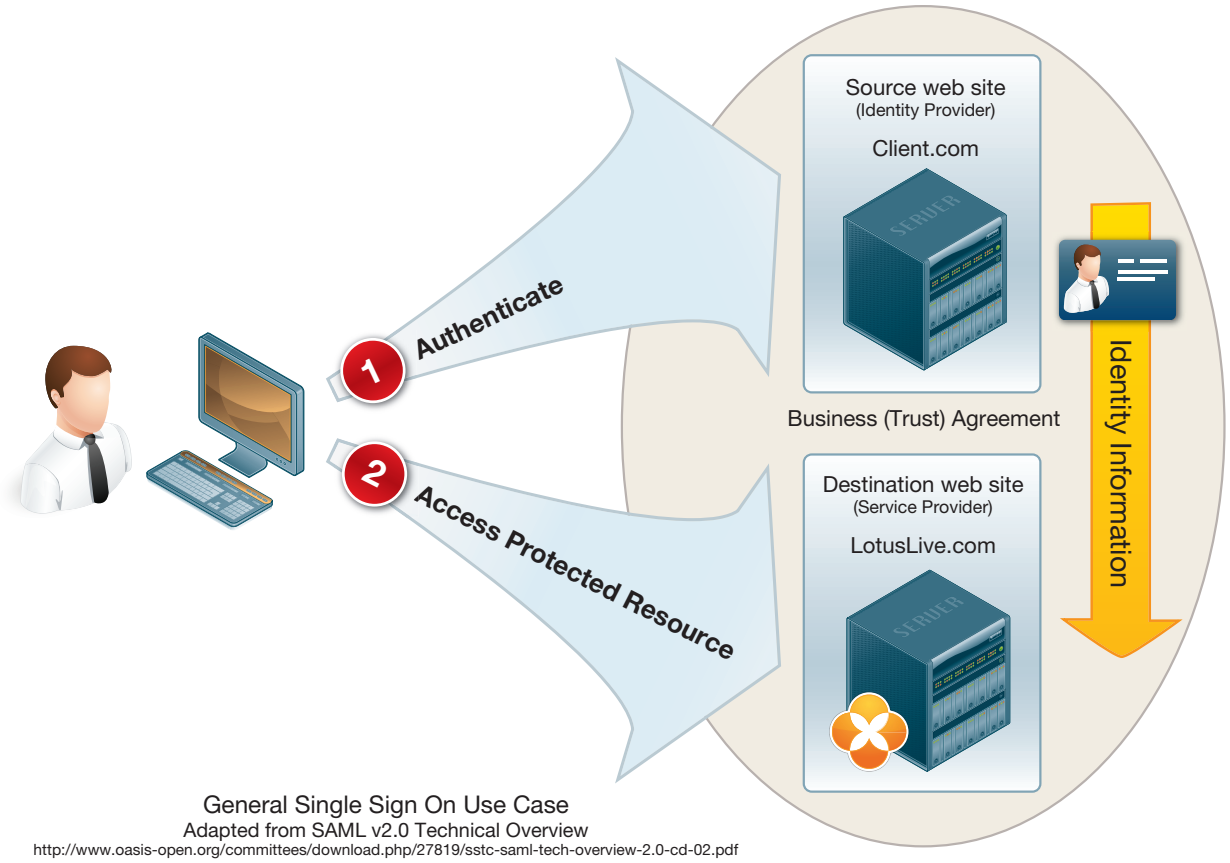
1.1. What is Federated Identity?

Federated identity is a general term that encompasses details regarding how two or more organizations wish to share identity information. A federated identity implementation usually consists of a single system, the Identity Provider, which authenticates a user and then vouches for the user's identity to other systems which do not have access to the user's authentication credentials.

Federated Identity is based on a trust relationship between an Identity Provider and a Service Provider. The Identity provider owns the user identities, controls the authentication of these identities, and provides identity information. This would normally be a directory server on the client's premises, such as Tivoli or Active Directory. The Service provider controls access to services, trusts asserted identity information provided by the Identity Provider, and provides access based on the asserted identity. This is LotusLive.

The most common use of federated identity is Multi-Domain Single Sign On (MDSSO), or more simply, SSO. In the general case, as a user moves from one domain (web site) to another, the source site provides a token to assert that the user is valid, and the destination site, based on the existence of a previously defined trust relationship with the source, accepts this assertion (once it's verified that it's genuine) and allows the user access.

1 Introduction to Federated Identity



General Single Sign On Use Case
Adapted from SAML v2.0 Technical Overview
http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

The movement between sites may be explicit (i.e. the user recognizes that the site is changing) or not. The important thing is that the user is not asked to log into the destination site.

How the first site authenticated the user is not important to the exchange of the identity information and assertion. The user could have authenticated using a username & password combination, through a token based authentication system, a network password, or because access is being requested from within a secure location. The first site considers the user valid, so it asserts to the second site that this is a valid user, and the second site accepts this assertion based on the fact that it trusts the source.

It is important to note that when Federated Identity is selected, both systems must be reachable by the user in order for a user to access LotusLive. If your Identity Server can't be reached, there will be no way to authenticate the user, and they will not be able to access LotusLive services.

LotusLive currently supports federated identity with outside parties using the Security Access Markup Language (SAML 1.1). SAML is an open standard created by OASIS (www.oasis-open.org), a non-profit consortium dedicated to the creation of open standards for information security.

1 Introduction to Federated Identity

Clients who create an identity federation with LotusLive would be able to authenticate their users however they wish, as long as they meet an acceptable minimum standard, using any mechanism they want, from passwords to Kerberos. Similarly, if a company has VPN or in-office-only access restrictions to the location of the login page, these restrictions are effectively inherited by LotusLive because users need to access the login page first. LotusLive does not need to have your user's passwords and no synchronization with LotusLive is needed when users change their password on the company directory.

1.2. Why SAML?

There are a number of competing approaches to Federated Identity, including both proprietary and open standards. Clearly proprietary standards are inappropriate for SaaS offering, and amongst the various alternatives SAML is widely considered the leading choice. In 2007, Gartner, an industry analyst firm, declared SAML 2.0 "the de facto federation standard across industries."[1]

The Federated Identity services embedded within LotusLive are provided by the Tivoli Federated Identity Manager (TFIM) which has the capability to accept identity tokens in a number of formats, including SAML 2.0, OpenID, and WS-Federation. Thus, a choice existed. SAML 1.1 was chosen over the others due to a combination of factors including its wide spread availability, security concerns raised about some of the alternatives, and ease of implementation for our clients.

Federated Identity using SAML is supported by a wide range of commonly used directory servers, including:

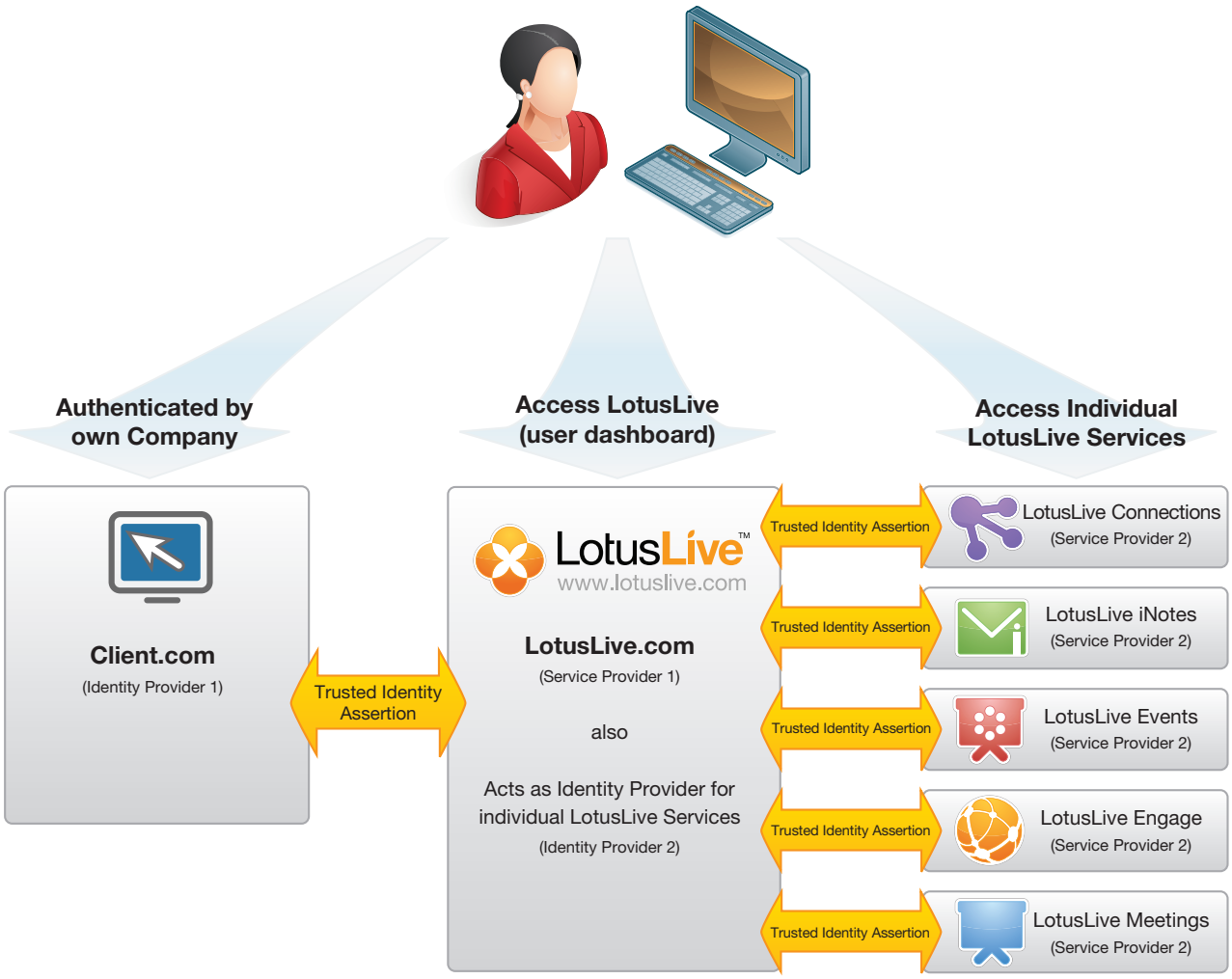
- Tivoli (TAM/TFIM)
- Active Directory (from Windows Server 2003 R2)
- Novell
- Sun Federated Access Manager (formerly Sun Access Manager & Sun Federation Manager)
- CA Federation Manager
- And others.

1.3. Identity Daisy Chains

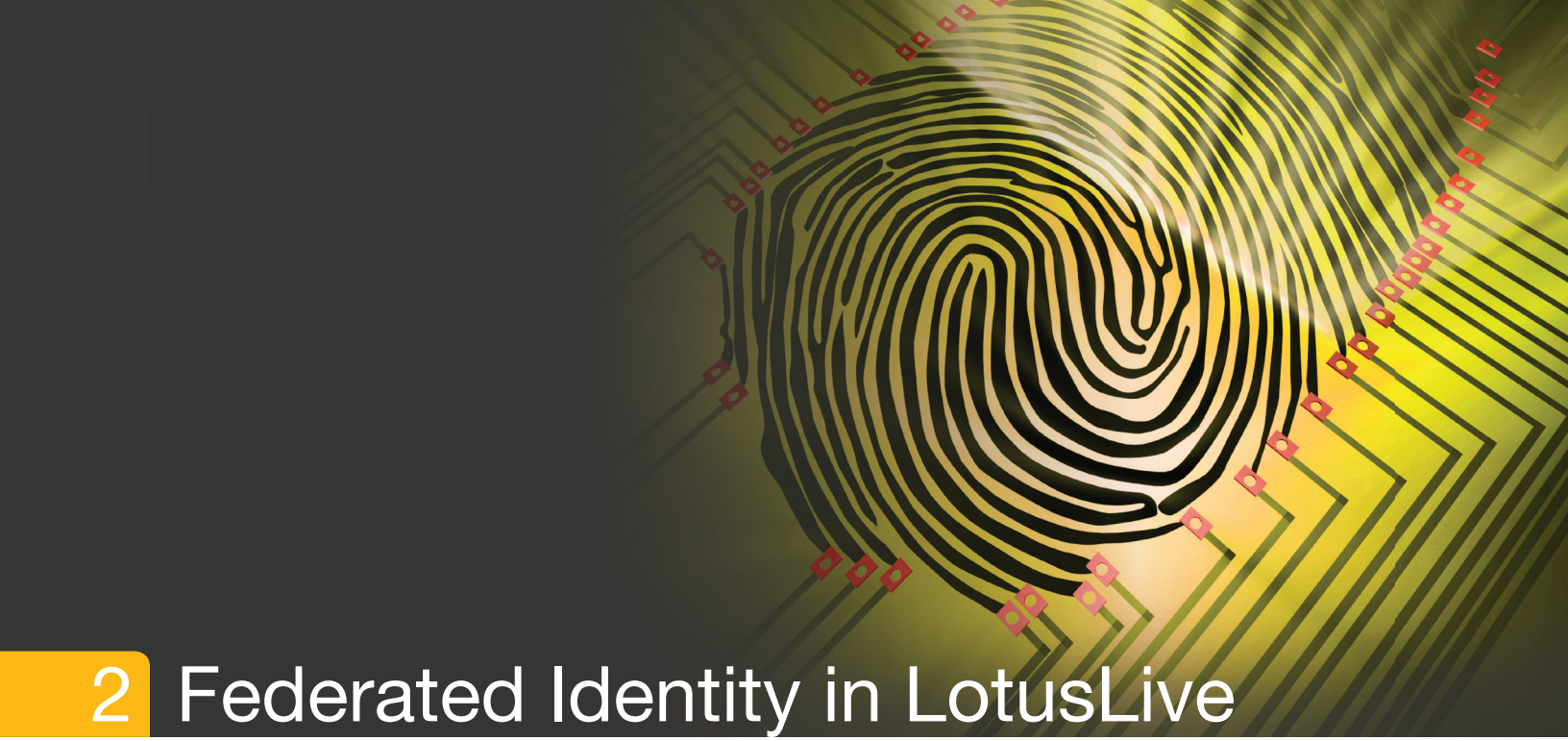
One of the advantages of Federated Identity, is that once a system is certain that a user is who he claims to be, the Service Provider can, in turn, become an Identity Provider to other Service Providers. This allows LotusLive, for example, to provide an assertion of identity that allows users to access the component services within LotusLive regardless of where a service is physically located, or whether or not it can share the LotusLive domain or, like with the email services, operates using the client's domain. Any

[1]Source: Gartner, Inc. "The U.S. Government's Adoption of SAML 2.0 Shows Wide Acceptance", by Gregg Kreizman, John Pescatore and Ray Wagner, October 29, 2007

current or future service (including third party services) that may be offered as part of LotusLive can be linked in this manner, allowing users to move between them seamlessly. It doesn't matter which service the user starts his session with, or how he might move around between services, as long as the first authentication came from the user's primary Identity Provider – his or her company.



LotusLive Internal Identity Federation



2 Federated Identity in LotusLive

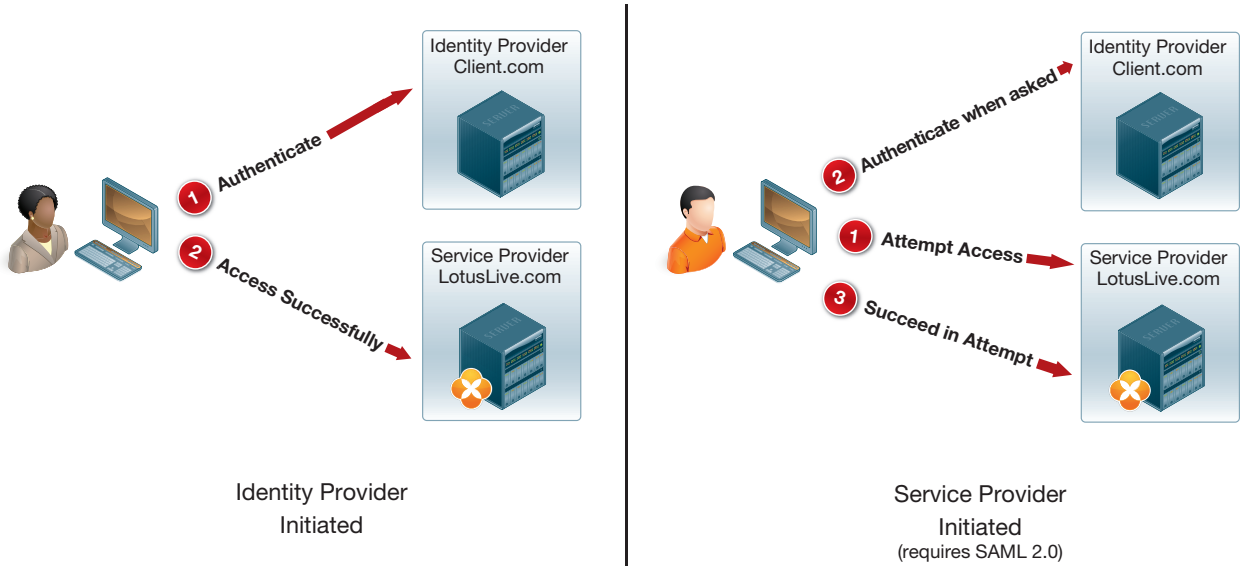
2.1. Who initiates the process?

The current public SAML specification (SAML 2.0) defines two options. The first is referred to as the Identity Provider Initiated model (IdP-Initiated), the second the Service Provider model (SP-Initiated). LotusLive currently implements SAML 1.1, and the IdP-Initiated model only, in which the user must first go to his Identity Provider, and the Identity Provider is responsible for redirecting the user's browser to the Service Provider (LotusLive), with the SAML assertion of identity, once the user has been authenticated.

What this means, in practical terms, is that clients using Federated Identity with LotusLive must provide one or more starting points for their users to access LotusLive services. A starting point can be an explicit login page, or could simply be a link on a company Intranet site. The starting point could require the user to (re)authenticate, or it could know that the user must have been authenticated in order to have arrived at that point. A company could provide both an internal starting point that does not require the user to enter a user name and password, as well as an external one that does – or can use other means to determine if the user has already been authenticated and decide whether or not to require a password at that time. If the Identity Provider requires more than just a name and password in order to authenticate on their end, then by extension LotusLive access is protected by the same security measure.

Users of federated identity who go directly to www.lotuslive.com will not be able to log in, and LotusLive will not be able to redirect them to their appropriate starting points.

2 Federated Identity in LotusLive



Differences in Initiation of Web Browser SSO
Adapted from SAML v2.0 Technical Overview
http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

The SP-Initiated model is only available in SAML 2.0, which is not yet supported.

2.2. Identity Federation Types

SAML doesn't solve everything, notably in the context of email. The established protocols for POP, IMAP & SMTP , as well as Lotus Sametime, do not support Federated Identity concepts very well. To help overcome these limitations of these older, established, mail protocols, LotusLive offers several federation configuration options:

2.2.1. Organization Types

- **Non-Federated:** An organization in which all subscribers will authenticate with a username and password stored in LotusLive. In this case SAML SSO is not being used.

- **Federated:** An organization in which all subscribers must authenticate with their organization's Identity Provider. Users cannot change their password inside LotusLive. In this case SAML SSO is being used.

- **Modified:** An organization that will allow all subscribers to authenticate with a username and password stored in LotusLive or their organization's Identity Provider. In this case SAML SSO is being used, but is optional.

- **Partial:** An organization can have subscribers that are Non-federated, Federated, or Modified. In this case SAML SSO is being used, but if and how it is to be used is set individually for each user.

The difference between Modified and Partial is that in a Modified organization all users have the option to use either authentication mechanism at any time. E.g. a user clicking through from the company Intranet may be automatically signed on using SAML, but going directly to www.lotuslive.com from home will be allowed to log in with their user ID and password. Organizations defined as Partial have users who carry one of the explicit designations below, which controls the authentication process for the individual user.

2.2.2. User Types

- **Non-Federated:** These are subscribers that use a username and password to authenticate directly with LotusLive. These users cannot use single sign on.

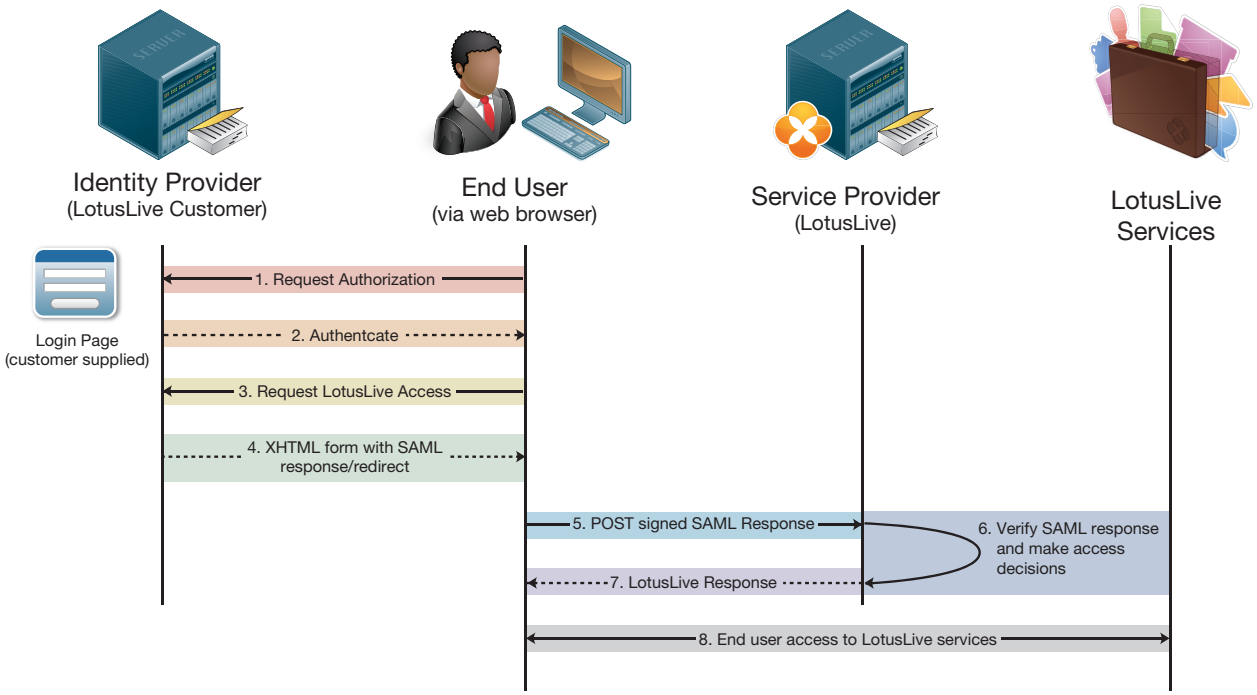
- **Federated:** These are subscribers that will not have a password in LotusLive and must authenticate via their organization's Identity Provider. For these users SAML single sign on is mandatory.

- **Modified:** Subscribers of this type will be able to authenticate both with passwords stored in LotusLive or by using their organizations Identity Provider via SAML single sign on.

The Federation type for the organization should be specified at the time the service is initially configured, as it will impact the process of user on-boarding (e.g. federated users will not be asked to supply an initial password), although it can be changed later.

2.3. How SAML works

2.3.1. The authorization conversation



1. User accesses their organization's intranet.
2. User authenticates with their organization's intranet using organizational standards for user authentication.
3. User requests access to LotusLive. Typically this will happen by the user accessing an HTML page that contains links to federation partners.
4. The user selects the LotusLive federation. The SAML token is then created by the identity provider and passed to the user's web browser.
5. The user's web browser is then redirected to the LotusLive federation endpoint and the SAML token is submitted via a form.
6. The SAML token is verified by LotusLive and access to LotusLive content is created for the user.
7. Secured LotusLive content is then sent back to the user's web browser.
8. User begins to interact with the LotusLive services

2.3.2. Trust Data Provided by the Identity Provider to the Service Provider

SAML is based on a private/public key system, so the key element of the trust relationship is the exchange of the public key, so the SAML tokens can be decoded and the signature validated by LotusLive. In order to establish the necessary trust relationship clients need to supply to IBM:

- **Identity Provider Company Name**
- **Contact Person:** First and last name, email, phone
- **Provider ID:** This is another name for the issuer element that can be seen in the SAML token example below. Typically, it is set as the URL where the assertion is being sent from, but this can be any string. The purpose of this value is just another way to verify by whom the token was generated.
- **Intersite transfer service:** The endpoint (a URL) on the identity provider point of contact server where the sign-on request process begins. This is the location to which users' single sign-on requests are sent if the user arrives at the service provider's site first (as outlined in section 2.1).*
- **Artifact resolution service end point.***
- **The public key** that belongs to the private/public pair that is used to generate the digital signature placed in the SAML assertion.

> * These two entries are optional in the current implementation, as they are used for functions that are not yet supported. However entries are need for these fields when setting up the Federation. As they are usually set up anyhow when an IdP is created, if the real values are available its best to have them in the system for potential future use.

The public key certificate associated with the private key that is used to sign the SAML messages created by the identity provider, as well as other aspects of the initial exchange of encrypted data. These data elements are highlighted in the XML metadata file sample that follows in corresponding colors.

2.3.3. Public Key & Trust Data Exchange

The public key and trust data described above can be provided in one of two ways to IBM. The first way is for the information to be sent in raw format (in a Java Key Store). The second option for providing the partnership information is as part of a SAML metadata file. The implementation in the LotusLive environment will allow the metadata file standard defined by SAML 2.0 to be imported. If you have an implementation that exports meta data the public key will be in it. Below is an example SAML metadata file for a SAML 1.1 identity provider. The highlighted URLs in the example below will be specific to each identity provider, and need to be set according to the local IdP configuration.

```
<?xml version="1.0" encoding="UTF-8" ?>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        entityID="https://ghvmdev019.clientco.com/FIM/sps/SAML/saml11">
    <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
        <md:KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
                    <X509Certificate>...public key goes here...</X509Certificate>
                </X509Data>
            </KeyInfo>
        </md:KeyDescriptor>
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP- binding"
        Location="http://ghvmdev019.clientco.com/FIM/sps/SAML/saml11/soap" index="0"
        isDefault="true" />
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
            Location="http://ghvmdev019.clientco.com/FIM/sps/SAML/saml11/login" />
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-
                post" Location="http://ghvmdev019.clientco.com/FIM/sps/SAML/saml11/login" />
            </md:IDPSSODescriptor>
        <md:Organization>
            <md:OrganizationName xml:lang="en">ClientCo</md:OrganizationName>
            <md:OrganizationDisplayName xml:lang="en">ClientCo
            </md:OrganizationDisplayName>
            <md:OrganizationURL xml:lang="en">https://ghvmdev019.clientco.com/FIM/LLFITest
            </md:OrganizationURL>
        </md:Organization>
        <md:ContactPerson contactType="technical">
            <md:Company>ClientCo</md:Company>
            <md:GivenName>John</md:GivenName>
             <md:SurName>Smith</md:SurName>
            <md:EmailAddress>jsmith@clientco.com</md:EmailAddress>
            <md:TelephoneNumber>1-555-123-4567</md:TelephoneNumber>
        </md:ContactPerson>
    </md:EntityDescriptor>
```

2.3.4. Constructing the SAML token

LotusLive accepts SAML 1.1 tokens. These tokens should be signed by an XML signature method and contain the email address of the user who is being authenticated. The SAML assertion contains 5 major parts that will be expected in the SAML assertions provided to the LotusLive endpoint. These five parts are highlighted in the sample token below, and can be defined as:

1. **Issuer** – Identifier for the Identity Provider
2. **Signature** – Digital signature of the Identity Provider
3. **Subject** – Identifies the authenticated principal
4. **Conditions** – States the conditions under which the assertion is valid
5. **AuthnStatement** – Describes how authentication was performed on identity provider

Presently LotusLive's Federated Identity only requires an assertion of the user's email. This email assertion will be used by LotusLive to provide access to the user's account for all services.

The typical scenario will be for the identity provider will be to provide the user's email as the subject of the message. The LotusLive environment allows for XML transformations which will allow the user email to be extracted from any part of the SAML token, but the email must be included in the token based on LotusLive's current implementation.

LotusLive does not require any additional KeyInfo elements in the XML signatures written to the SAML token. These xml elements will be ignored if included because LotusLive requires the Public Key to be provided when partnership is setup.

2.3.5. Sample SAML token

Here is an example XML SAML token that will be acceptable for LotusLive federation identity:

```
<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" IssueInstant="2009-06- 10T20:20:21Z" MajorVersion="1" MinorVersion="1" Recipient="https://apps.lotuslive.com/sps/sp/saml11/login" ResponseID="FIMRSP_cbd4130a-0121-12af b299-fbc-c161dfd41">
    <ds:Signature Id="uuidcbd4130b-0121-13c2-85f7-fbcc161dfd41">
    ...
    Digital signature of the Identity Provider goes here
    …
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success" />
    </samlp:Status>
    <saml:Assertion AssertionID="Assertion-uuidcbd41304-0121-1088-bca7-fbcc161dfd41"
        IssueInstant="2009-06-10T20:20:21Z" Issuer="https://ghvmdev019.clientco.com/FIM/sps/SAML/saml11" MajorVersion="1" MinorVersion="1">
        <saml:Conditions NotBefore="2009-06-03T21:40:21Z" NotOnOrAfter="2009-06-17T19:00:21Z">
            <saml:AudienceRestrictionCondition>
                <saml:Audience>https://apps.lotuslive.com/sps/sp/saml11</saml:Audience>
            </saml:AudienceRestrictionCondition>
        </saml:Conditions>
        <saml:AuthenticationStatement AuthenticationInstant="2009-06-10T20:20:21Z"
            AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
            <saml:Subject>
                <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.0:assertion#email
                    Address"> jsmith@clientco.com</saml:NameIdentifier>
                <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer
                    </saml:Confir mationMethod>
                </saml:SubjectConfirmation>
            </saml:Subject>
        </saml:AuthenticationStatement>
    </saml:Assertion>
</samlp:Response>
```

2.3.6. The SAML Form Post

The identity provider creates a form that is posted to the LotusLive SAML endpoint. Here is an example form that is used by TFIM:

```
<!DOCTYPE HTML PUBLIC “-//W3C//DTD XHTML 1.1//EN” “http://www.w3.org/TR/xhtml11/
DTD/xhtml11.dtd”>
<html xml:lang=”en” xmlns=”http://www.w3.org/1999/xhtml”>
    <head>
        <script language=”JavaScript”>
            <!--
            document.cookie = “IV_JCT=%2FFIM; path=/”;
            //-->
        </script>
        <meta http-equiv=”Content-Type” content=”text/html; charset=UTF-8”>
        <title>SAML POST response</title>
    </head>
    <body>
        <form method=”post” action=”https://apps.lotuslive.com/sps/sp/saml11/login”>
            <p>
                <input name=”TARGET” value=”https://apps.lotuslive.com” type=”hidden”>
                <input name=”SAMLResponse” value=”PHNhbWxwOlJlc3BvbnNlIHhtbG5zOmRzP
                SJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIiB4bWxucz
                pzYW1sPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoxLjA
                .
                This is the encoded XML SAML token
                .
                WZpY2F0ZT48L2RzOlg1MDlEYXRhPjwvZHM6S2V5SW5mbz48L2RzOlNp
                Z25hdHVyZT48L3NhbWw6QXNzZXJ0aW9uPjwvc2FtbHA6UmVzcG9uc2U+“
                type=”hidden”>
                <noscript>
                    <button type=”submit”>POST</button>
                    <!-- included for requestors that do not support javascript -->
                </noscript>
            </p>
        </form>
        <script type=”text/javascript”>
            var signOnText = ‘Please wait, signing on...’;
            document.write(signOnText);
            setTimeout(‘document.forms[0].submit()’, 0);
        </script>
        Please wait, signing on...
    </body>
</html>
```

2.4. LotusLive's SAML Endpoints

The LotusLive SAML endpoint, where SAML token is posted to once the Identity Provider has authenticated the user, is:

https://apps.lotuslive.com/sps/sp/saml11/login

The LotusLive target is (where the user's browser is then redirected to):

https://apps.lotuslive.com

LotusLive federated identity support assumes communication between the Identity Provider and LotusLive over public internet. SSL 3.0 is used to secure this communication channel.

2.5. Identity Provider SLA Responsibility

Clients opting for federated identity must recognize that their system is a critical component of access to the LotusLive system. Their users will not be able to access LotusLive services, which may include their mail boxes, if the Identity Provider (IdP) service is down or cannot be reached for any other reason. The customer is responsible for providing a logon page and the SAML IdP which achieves an SLA at least as good as the contract SLA for the services. Outages of the customer provided login page and SAML IdP shall be excluded from any SLA availability calculation.

2.6. Using More Than One Identity Provider Source

If your organization has more than one directory server for the same domain they do not necessarily need to be consolidated into one Identity Provider (IdP). LotusLive Federated Identity can accept tokens from multiple IdPs on the same domain, as long as they are all signed with the same digital signature.

However, if this is necessary, it is advisable to bring this up early in the process so the compatibility of your IdP layout, with LotusLive, can be validated prior to starting the implementation.

3 Project Steps & Readiness Checklist

Here is a brief outline of the steps, and items needed, to get Federated Identity set up. Any of these steps may need to be expanded, in your environment, into a small project to prepare the system. A readiness assessment should be done in advance of planning an implementation of Federated Identity, following this list.

- Are you currently using a directory server, such as TDS or AD, and is your directory server ready to support SAML based Federated Identity?

- Are your users all using/on the (or a) directory server? While it is not necessary for all users to be on a consolidated directory, if users are widely distributed over many servers (or some users are not on any) then it will be worth investigating the impact of directory consolidation before trying to set up Federated Identity.

- If you are using multiple directory servers, are any in remote locations that will have slow or un-reliable connections to where remote users of LotusLive might be logging in from? If access to a directory in Peru is unreliable from New York, this is not necessarily a problem if the server will be reliably available to employees in Peru. On the other hand, if a server in New York is hard to reach for mobile employees who are on assignment in Peru, it may be preferable not to federate those users. This step can help you determine what federation type you will need to set up.

- Are there any reasons (e.g. security, network configuration) that would prevent your directory server from being reached from outside the firewall, to provide the necessary service? If security concerns will prevent your primary directory from being reachable for all the necessary cases,

consider mirroring only the necessary data set onto another directory server that can be placed in a position with the necessary access available.

- Does the directory server hardware (and network) have capacity to accept the additional work-load?

- As the Identity Provider, your set up should be complete, and tested, before providing your trust relationship data to IBM. An end to end test can be performed by setting up a dummy service provider on spare hardware either using your existing software (i.e. the same directory server) or by downloading and setting up a free implementation from a source such as OpenSAML (see links in next section).

- Purchase the necessary certificates. Although self-signed certificates can be used, and are good for testing, browsers react badly to them and can confuse users with dire sounding warnings, and repeated requests to trust the certificate.

- Add LotusLive as an allowed service for SAML authorization.

- Supply the trust relationship information package to IBM

4 Additional Resource Links

4.1. Setting up Federated Identity for specific systems

The following links may assist you in finding the information you need to set up SAML services with a number of the directory servers in the market today. These links are provided for your information only. Please consult your product's manuals.

4.1.1. Tivoli Federated Identity Manager

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.tivoli.fim.doc_6.2/welcome.htm

http://www.redbooks.ibm.com/abstracts/sg246014.html?Open

http://www.redbooks.ibm.com/abstracts/sg246394.html?Open

http://www.redbooks.ibm.com/abstracts/redp3678.html?Open

http://www.redbooks.ibm.com/abstracts/redp4354.html?Open

4.1.2. Microsoft Active Directory Federation Services

ADFS Deployment Guide:

http://technet.microsoft.com/en-us/library/cc758030(WS.10).aspx

Implementing Your ADFS Design Plan:

http://technet.microsoft.com/en-us/library/cc782250(WS.10).aspx

Others:

http://www.microsoft.com/downloads/details.aspx?familyid=062F7382-A82F-4428-9BBD-A103B9F27654&displaylang=en

http://msdn.microsoft.com/en-us/magazine/cc163520.aspx
http://technet.microsoft.com/en-ca/magazine/2006.07.simplify.aspx

4.1.3. Sun Access Manager

http://developers.sun.com/identity/reference/techart/sso.html

4.1.4. Novell

http://developer.novell.com/wiki/index.php/Novell_SAML_Toolkit

4.1.5. CA Federation Manager

https://support.ca.com/irj/portal/anonymous/DocumentationResults

4.2. General FID/SAML Resources

Wikipedia entry for a basic explanation of SAML

http://en.wikipedia.org/wiki/SAML

Oasis Group, the origin of SAML:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
http://www.oasis-open.org/committees/security

Online community and information resource for the SAML OASIS Standard:

http://saml.xml.org/

OpenSAML – Open source SAML libraries in Java and C++.

http://www.OpenSAML.org/

Presentation on SAML 2.0

http://www.parleys.com/display/PARLEYS/Home#talk=7602261;slide=1;title=SAML%20v2

Presentation on SAML

http://www.infoq.com/presentations/saml