MLSListings Single Sign On Implementation Guide

Compatible with MLSListings Applications

February 2010

TABLE OF CONTENTS

Introduction

This document describes SAML SSO integration at MLSListings. The SAML SSO interface is available for MLSListings partners and third-party vendors who wish to integrate with MLSListings applications.

This chapter includes information on the following topics:

- Introduction to MLSListings SSO
- Using the SAML SSO Standard
- Benefits of Using SAML SSO Authentication
- Who Should Use this Guide
- Organization

Introduction to MLSListings SSO

In simple terms, SSO enables users who login to (authenticate with) a partner application to have access to MLSL applications without requiring another login. In turn, users who login to (authenticate with) MLSL applications have access to MLSL partner applications without requiring another login.

Examples of SSO applications supported by MLSListings Inc. include:

- Realist Tax Information (hosted by Realist.com ®)
- MLSListings Matrix (hosted by Tarasoft ® Corporation)
- MLSListings California Edition

Using the SAML SSO Standard

To create Single Sign On (SSO) integrations with partners and vendors, MLSListings requires using the Security Assertion Markup Language (SAML Version 2). By designing to a common SSO standard, MLSListings partners and vendors have a well-defined and efficient procedure for making login authentication compatible across products.

SAML is an XML-based framework for exchanging authentication and authorization data between an *identity provider* and a *service provider*:

- A service provider is a business that provides subscription or web services to other businesses or individuals.
- An identify provider is a special type of service provider that creates, maintains, and manages identity information for users and provides user authentication to other service providers.

The SAML standard is defined by the Organization for the Advancement of Structured Information Standards (OASIS). You can find the latest specifications, forums, and additional documentation published by the OASIS Security Services Technical Committee at the OASIS site (http://www.oasis-open.org/).

Note: For a brief overview of the SAML SSO standard and description of the SAML SSO process, see Chapter 1 of this document.

Benefits of Using SAML SSO Authentication

Some benefits of using SAML SSO authentication include:

- A consistent interface for SSO integration.
- SAML is a well-defined, industry standard.
- Vendors and partners can use their own authentication methods and still provide an SSO interface with MLSListings applications.

Who Should Use this Guide

This document is intended for MLSL partners (software developers and IT professionals) who are responsible for setting up access to the MLSListings applications and for enabling MLSL users to access their partner applications.

To work with the MLSListings SSO interface, you should have experience in the following areas:

- Networking, web development, and HTTP
- Familiarity with the SAML standards
- Microsoft technologies and platforms including Windows Server, SQL Server, Internet Information Services (IIS) and the Microsoft .NET framework.

Organization

This document is organized into the following parts and chapters:

- Chapter 1: “Introduction to SAML SSO”

  This chapter provides some background material on the SAML SSO standard and provides a description of how the SAML SSO authentication process works.

- Chapter 2: “SAML Integration at MLSListings”

  This chapter describes how SAML SSO integration as implemented at MLSListings Inc.

- Chapter 3: “Glossary”

  This section contains a list of commonly used SAML SSO terms.

- Appendix

  This appendix includes sample files and support information for your reference:

  - MLSListings SAML Metadata
  - SAML <AuthnRequest>
  - SAML <Response>
  - SAML <Response> with Impersonation

1

Introduction to SAML SSO

This chapter provides background material on the SAML SSO standard and provides a description of how the SAML SSO authentication process works. Topics include:

- About the SAML SSO Standard
- The SAML SSO Process – An Example

If you are already familiar with SAML SSO authentication, you can skip ahead to Chapter 2, “SAML Integration at MLSListings.”

About the SAML SSO Standard

In the past, Single Sign On solutions were abundant at the intranet level. However, extending these solutions beyond the intranet has been difficult and has led to the proliferation of incompatible, proprietary technologies. To solve this problem, SAML has become the definitive standard underlying many web Single Sign On solutions for enterprise applications.

SAML assumes the *principal* (typically a user or subscriber) has enrolled with at least one *identity provider*. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services. This makes SAML a valuable, flexible tool because a *service provider* (typically a web application that provides a service to the principal) can rely on an identity provider to identify the principal without being dependant on the means the identity provider uses to make the identification.

This is an implementation of *federated trust*. The organization owning an identity provider does not need to be the same organization owning a service provider that depends on that identity provider for authentication services. When requested to authenticate a user, an identity provider first establishes the identity of the user by some method of secure authentication and then sends the service provider an *assertion* which is a statement of fact describing the authentication. For example "This user has been identified as John Doe using Arcot strong authentication." The assertion also identifies the organization providing it and is usually signed to prevent tampering. The service provider does not independently authenticate the user; it *trusts* the identity provider to provide a truthful assertion and grants the user access to the service based on this assertion. This trust is based on a business arrangement between the organizations.

A SAML assertion is a statement of fact, not a demand for access. The service provider can allow full or restricted access or deny access based on the information in the assertion. For example, if the arrangement between the business organizations requires strong authentication, the identity provider may still send an assertion saying that a particular user has been authenticated using username and password only. The service provider may then deny access based on the lack of strong authentication. In a correct implementation of federated trust, the sender of an assertion must always send one that is factually correct and the receiver must check that it meets all acceptable criteria before granting access.

The SAML SSO Process – An Example

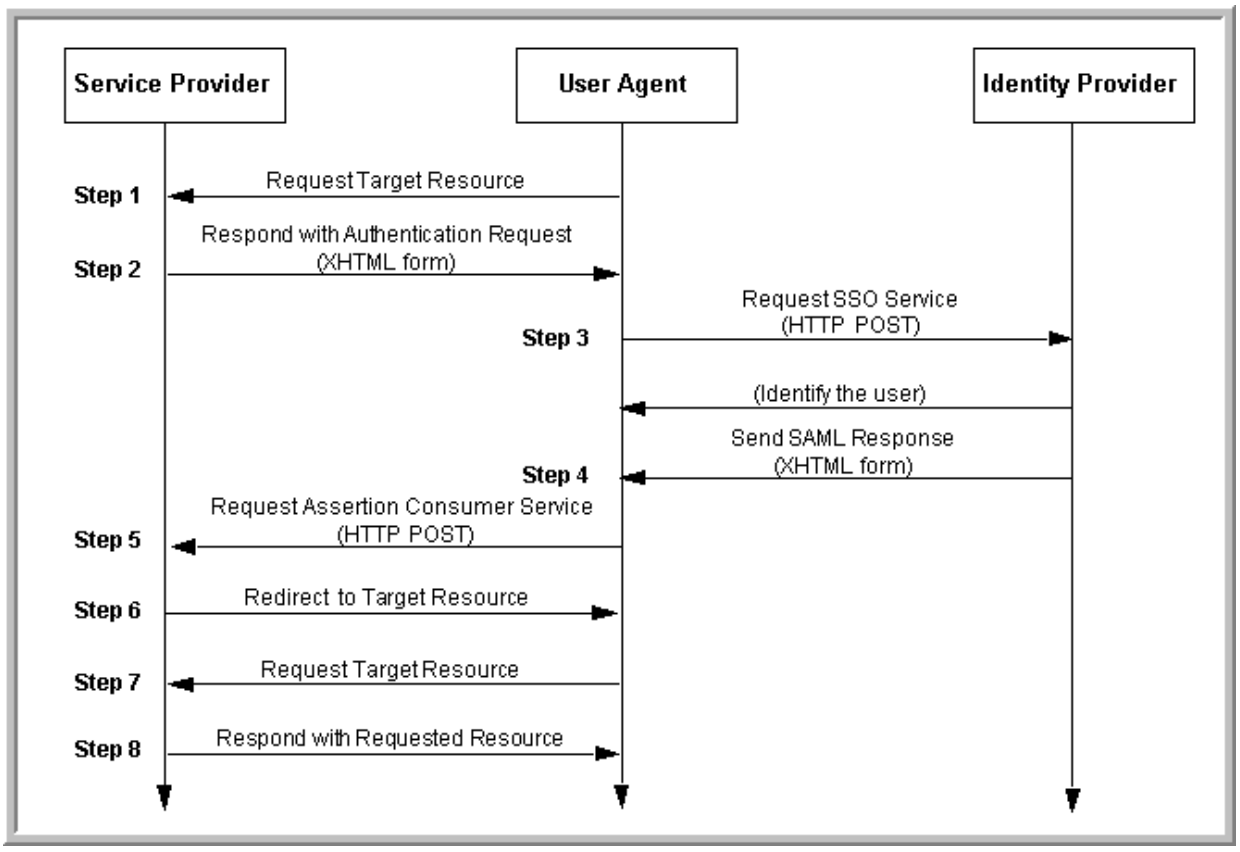
MLSListings implements the Web Browser SSO Profile described in *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. In simple terms, this SAML profile defines how SAML authentication requests and responses are transmitted using a combination of HTTP Redirect and HTTP POST bindings.

SAML allows one or more identity providers to interoperate with one or more service providers. For example, the users of a service provider can be divided into several communities, each of which is authenticated by a different identity provider. Or, several service providers can be shared by the same community of users who are authenticated by an identity provider. If the same user uses more than one service provider simultaneously or in sequence, he does not need to authenticate more than once. Once his identity has been established by the identity provider, the same credentials can be passed to all of the service providers. This is the basis of SSO.

SAML allows a sign on to be initiated by either a service provider or an identity provider. Currently, In the MLSListings implementation, we have chosen to have the service provider initiate a sign on. However, in the future, MLSListingscould also implement identity-provider-initiated sign on if needed. In service-provider-initiated sign on, the user, by means of a *user agent* (typically, a web browser), requests a web resource protected by a SAML service provider. If the service provider requires a user to authenticate, it issues a SAML <AuthnRequest> to an identity provider. The means by which an identity provider is chosen for each user is not specified by the SAML specification.

The identity provider determines the identity of the user by whatever means are appropriate. Typically, this includes prompting the user to enter a username and password or a secure token code. However, if the identity provider already has active credentials for the user, it may simply return those credentials with no user action required. To return the credentials, the identity provider sends a SAML <Response>. This response contains an authentication assertion (if the use provided the proper authentication information) or an error (if the use did not provide the proper authentication information). The service provider uses information in the SAML <Response> to establish a security context (login permission, account access, and so on) or report an error.

Figure 2: SAML Sign On Process Flow [1]



Step 1. The principal (user), by means of an HTTP user agent (typically, a web browser) requests a target resource at the service provider.

This request may be the first request for a resource by this user, but more typically the user has already signed into a service provider (application) and is using it. That application has a means to request service from another service provider such as a hyperlink or button. The user requests access to the second service provider which initiates the sign in process.

The service provider initiates a security check on behalf of the target resource.

Step 2. The service provider responds with a document that contains an XHTML form. This is the authentication request <AuthnRequest>.

The authentication request specifies:

- Information about the subscriber who needs to be authenticated (user name, login, etc.)
- The name or ID of the identity provider who will perform the authentication.

[1] "SAML 2.0," Wikipedia, The Free Encyclopedia, November 2008.

Step 3. The user agent requests an Sign On service from the identity provider.

The user agent issues an HTTP POST request to the Sign On service at the identity provider where the value of the SAML request parameter is taken from the XHTML form mentioned in Step 2. The Sign On service processes the <AuthnRequest> and performs a security check.

Step 4. The SSO service at the identity provider creates or locates the credentials for the user. If it already has credentials for this user, due to a previous sign on, it simply returns them. If not, then it authenticates the user minimally by asking for information such as a username and password but often with a second factor as well such as a one-time password or a PKI certificate. The identity provider responds these credentials contained inan XHTML form. In addition to the user's credentials, the response describes the means of authentication and may also include additional implementation-specific attributes.

This is the SAML response <Response>.

Step 5. The user agent issues an HTTP POST request to the Assertion Consumer Service at the service provider.

The value of the SAML request parameter is taken from the XHTML form mentioned in step 4.

Step 6. The Assertion Consumer Service processes the response, creates a security context at the service provider and redirects the user agent to the target resource.

Step 7. The user agent requests the target resource at the service provider (again).

Step 8. Since a security context exists, the service provider returns the resource to the user agent, making it available to the user.

At this point, the user has access to the service provider and can use its functionality. The service provider application likely establishes a user session at this point which grants the user continued access to the service provider and additional requests for resources provided by the same provider within the scope of this session do not require another SAML authentication request.

2

SAML Integration at MLSListings

This chapter describes SAML integration as implemented at MLSListings Inc.

Topics include:

- Use Cases
- About the Implementation Process
- The MLSListings Staging Environment
- Web Browser SSO Profile
- MLSListings Acting as the Identity Provider
- MLSListings Acting as the Service Provider
- SAML Subject and Attributes
- SAML Metadata
- SAML Certificate and Samples

Use Cases

A SAML SSO project implements one or both of the following use cases:

1. A vendor wishes to grant access to its application to MLSListings's subscribers directly from MLSListings's applications. Subscribers are authenticated by MLSListings Connect implementation which is the MLSListings identity provider.
2. A vendor or partner wishes give access to an MLSListings service provider to a user community authenticated by the vendor or partner using an approved identity provider. MLSListings must approve the authentication method before such an arrangement can be allowed. The authentication methods allowed may vary depending on the service provider and scope of data being accessed, but typically MLSListings requires an industry-recognized form of strong authentication with at least two factors.

About the Implementation Process

To get started with a SAML SSO project, keep in mind the following:

- Vendors who wish to use MLSListings as an identity provider and who plan to automatically treat MLSListings subscribers as trusted, can implement SSO based on the information provided in this document.
- Vendors who wish to use MLSListings as a service provider must work with MLSListings to fully implement SSO. Information about vendor-side preparation is included in this document. However, to fully implement SSO, MLSListings must also qualify vendors systems identity providers and make configuration changes to allow those identity provider to access our service provider
- MLSListings supports browser-based SSO only.
- The sample files provided in this document are subject to change, contact MLSListings for the latest information.

The MLSListings Staging Environment

MLSListings Inc. supports a number of different internal and external deployment environments (DEV, QA, STAGING, PROD). The MLSListings Staging environment is a preproduction test platform. This environment is used for final testing before an application is taken "Live" in the Production (PROD) environment.

Vendors with signed partnership agreements can use the MLSListings Staging environment to test SSO implementations.

Important: All MLSListings examples and sample files mentioned in this document are designed for the Staging environment.

Accessing the Staging Environment

Public access to the Staging environment is granted only to current MLSListings partners and vendors who have a signed partner agreement. It is restricted to the specifically whitelisted public IP addresses of their corporate networks.

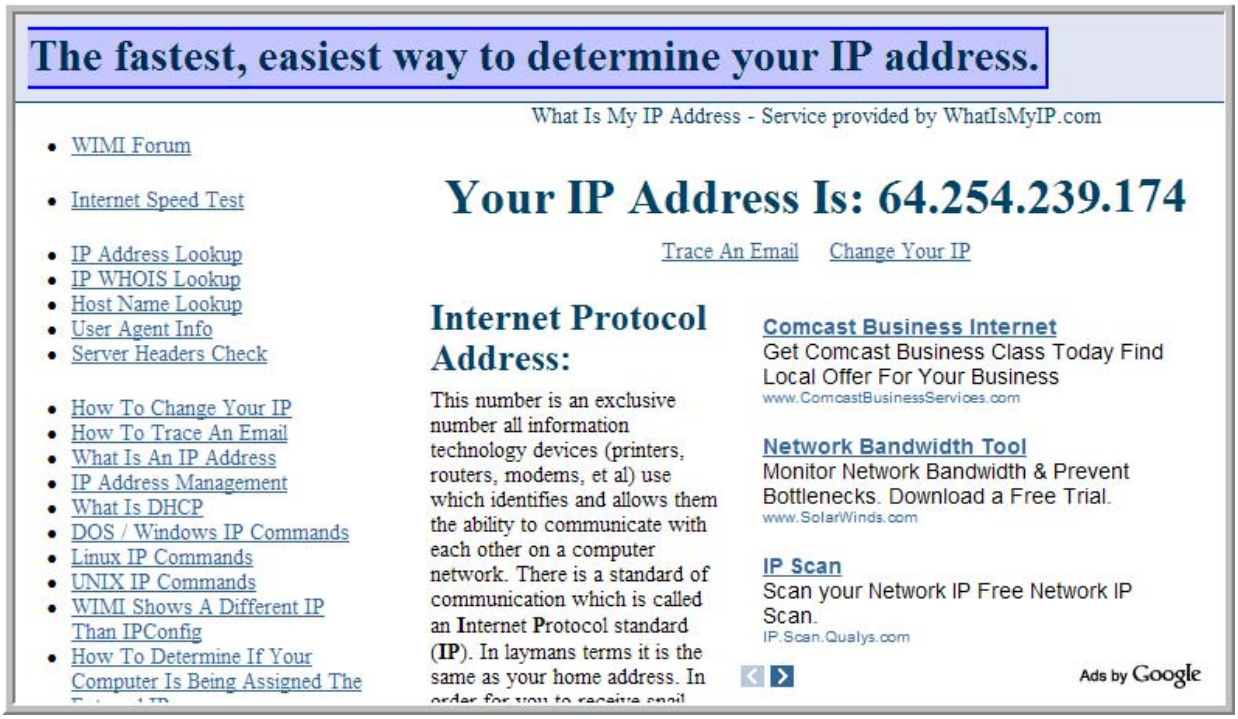
To apply for access to the MLSListings Staging environment:

- Determine the public IP address of your corporate network using web sites such as http://www.WhatIsMyIP.com or http://www.CheckIP.dyndns.com.
- Provide your public IP address to your designated Technical Support Representative at MLSListings.com. Your MLSListings contract will provide you with one or more test accounts.

  Each test account includes:

  Login Name
  Password
  Full Name

Figure 1: Determining Your Public IP Address



Service URLs in Staging

The following table shows service URLs available in the Staging environment.

Table 1: Service URLs in the Staging Environment

URL	Description
https://pro.staging.mlslistings.com	MLSListings Professional Edition
https://lm.staging.mlslistings.com	Listing Management
https://connect.staging.mlslistings.com	MLSListings Connect (authentication services)

Subscribers to MLSListings applications typically bookmark MLSListings Professional Edition.

SSL Certificates

MLSListings Inc. uses self-signed certificates in the Staging environment. These certificates should be installed locally to avoid browser warnings.

For reference, a copy of an SSL certificate for the Staging environment is available on the MLSListings Product Information page (Home > Reference Library > Product Information > SSO Integration).

Web Browser SSO Profile

MLSListings implements the Web Browser SSO Profile described in *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. This SAML profile defines how SAML authentication requests and responses are transmitted using a combination of HTTP Redirect and HTTP POST bindings.

MLSListings Acting as the Identity Provider

When MLSListings is the identity provider, it receives authentication requests at the following protocol endpoint:

`https://connect.staging.mlslistings.com/SAML/AuthnRequestResponder.ashx`

This handler supports both HTTP Redirect and HTTP POST bindings.

After receiving an authentication request, MLSListings determines the identity of the user and sends an SAML response to the service provider.

MLSListings Acting as the Service Provider

When MLSListings is the service provider, it issues authentication requests and receives authentication responses.

Issuing an Authentication Request

As a service provider, MLSListings issues authentication requests from the following handler:

https://connect.staging.mlslistings.com/SAML/AuthnRequestIssuer.ashx

The `AuthnRequestIssuer` handler supports one optional string parameter `idp` that specifies what identity provider to use. Values of the `idp` parameter are defined by MLSListings specifically for each SSO project.

For example:

https://connect.staging.mlslistings.com/SAML/AuthnRequestIssuer.ashx?idp=EastBay

sends authentication requests to a configured identity provider aliased as `EastBay` .

The URL for this endpoint is static and may be embedded in a hyperlink in a partner web application or bookmarked in a browser.

Note: If the `idp` parameter is empty or not supplied, the default identity provider is MLSListings. As mentioned above, MLSListings acting as an identity provider receives requests at:

`https://connect.staging.mlslistings.com/SAML/AuthnRequestResponder.ashx`

Receiving an Authentication Response

When MLSListings is the service provider, it receives the SAML <Response> at the following protocol endpoint:

`https://connect.staging.mlslistings.com/SAML/AssertionConsumerService.ashx`

SAML Subject and Attributes

When MLSListings is the identity provider, it is responsible for issuing a SAML <Response> that contains an <Assertion> that identifies the authenticated principal (the person).

The <Subject> of the SAML assertion is the login name of the authenticated principal. For MLSListings subscribers, the login name is typically an agent's 8-digit, California Department of Real Estate (DRE) number.

The AuthnRequestResponder will optionally return up to eight SAML attributes, including:

Table 1: SAML Attributes for MLSListings

Attribute Name	Description
FullName	The full name of the principal. For example, Benjamin Franklin. This attribute is usually present in the SAML response.
Email	The email address of the principal. For example, bfranklin@usa.gov. This attribute is usually present in the SAML response.
MLSDomain	The MLS Domain in which the principal initially authenticated. MLS Domains include: • MLSListings (MLSListings, Inc) • BARI (Bay Area Real Estate Information Services) • SACM (MetroList) • SFAR (San Francisco Association of Realtors) This attribute is usually present in the SAML response.
MLSMemberID	The MLS member identifier in the MLSD domain in which the principal initially authenticated. This may be an internal identifier in a membership management system. This attribute is usually present in the SAML response.
MemberOfficeRelationshipID	An internal identifier used in outbound SSO scenarios from MLSListings to a Quattro MLS. This attribute identifies the specific office that the authenticated principal should use. This attribute is usually **not** present in the SAML response.

EffectiveSubject	The login name of the effective principal which may be an impersonated identity. This will be the same as the <Subject> of the SAML assertion if impersonation is not in effect. This attribute is usually present.
EffectiveFullName	The full name of the effective principal which may be an impersonated identity. This will be the same as FullName if impersonation is not in effect. This attribute is usually present.
EffectiveEmail	The email address of the effective principal which may be an impersonated identity. This will be the same as Email if impersonation is not in effect. This attribute is usually present.

Applications (service providers) that support *impersonation* – one user working on behalf of another – can compare the SAML <Subject> with EffectiveSubject for equality to determine whether impersonation is active in the MLSListings authenticated session.

Applications that do not support impersonation can reliably use either SAML <Subject> to identify the true principal or the EffectiveSubject to identify the logical principal, depending on which identity is most appropriate to the application.

SAML Metadata

MLSListings provides SAML metadata that describes protocol endpoints and assertion contracts. Some MLSListings partners and vendors require this SAML metadata to configure SSO in their environments.

Current MLSListings SAML metatdata for the Staging environment is available any of the following locations:

https://connect.staging.mlslistings.com/SAML/

https://connect.staging.mlslistings.com/SAML/Default.aspx

https://connect.staging.mlslistings.com/SAML/MLSListings.xml

For reference, a copy of the metadata is also included in the Appendix of this document and a metadata file (MLSListings.xml) is available on the MLSListings Product Information page. (Home > Reference Library > Product Information > SSO Integration)

Important: The service endpoints and public keys in the SAML metadata vary depending on the MLSListings Deployment Environment (DEV, QA, STAGING, and PROD). The SAML metadata examples provided are for the STAGING environment.

SAML Certificate and Samples

The public key for the SAML certificate for the domain **`connect.staging.mlslistings.com`** is shown below:

```
-----BEGIN CERTIFICATE-----
MIIB+DCCAWWgAwIBAgIQFlD7lTTR6b1PzW8CEfrqXDAJBgUrDgMCHQUAMCoxKDAm
BgNVBAMTH2Nvbm5lY3Quc3RhZ2luZy5tbHNsaXN0aW5ncy5jb20wHhcNMDgxMDE1
MTgxNDEwWhcNMTgxMDEzMTgxNDEwWjAqMSgwJgYDVQQDEx9jb25uZWN0LnN0YWdp
bmcubWxzbGlzdGluZ3MuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa
jilkqzfELmMBrOBjbxFlyd8cI3FHjlhD1ULmUnoJ6xMuMaxI9hsGmB6ViSb5hGMA
x1+4AG57Ajsd1OjXW5Av0Bpr/tgGrH2iCUD4Q3lkODhy069UBtAfu7gnwsM/U5pt
FfWFtGVUYYwaFZP5nU2H3nNcEbq9tWD+J7TW1uDL8QIDAQABoycwJTATBgNVHSUE
DDAKBggrBgEFBQcDATAOBgNVHQ8EBwMFALAAAAAwCQYFKw4DAh0FAAOBgQCP/fp5
yDOs0BSysm9ml+He/StzuI1TEvovTcXqJaOdldWtIetq5cUIfN8PQ8kPjqXcC68C
8eyfPK8WqDoYjXE/qBoFE68h5fPe/ktunIFWx1VJtFP2MqAuA3q2v53xShET7MQP
s2YNQOUkgmN7qAMyaPNQPy45xNupFiYG2Ec7dQ==
-----END CERTIFICATE-----
```

For reference, a copy of the SAML certificate is available on the MLSListings Product Information page. (Home > Reference Library > Product Information > SSO Integration).

In addition to the certificate, a sample SAML <AuthnRequest> and a sample SAML <Response> are also provided.

3 Glossary

This chapter contains a list of commonly used terms for SAML SSO authentication.

Authenticate

Positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. For web applications, the process of identifying an individual is usually based on a username and password or security token.

HTTP Post

An HTTP Post is a type of HTTP request message. A POST is used when the requested action may change data on the server, such as updating data in a database or storing an uploaded file.

HTTP Redirect

On a web site, redirection is a technique for moving visitors to a different Web page than the one they request, usually because the page requested is unavailable or further processing is required.

Identity Provider (IdP)

A special type of service provider that creates, maintains, and manages identity information for users and provides user authentication to other service providers. A typical identity provider is an internet site which manages its own directory of user accounts.

Principal

A user (or subscriber) who requires authentication. Typically, a user authenticates by entering a username and password into a web browser.

Service Provider (SP)

A business that provides subscription or web services to other businesses or individuals. Examples of these services include internet access and web application hosting.

Single Sign On (SSO)

A service that enables a user to log in once and gain access to multiple, related, but independent software systems without being prompted to log in again at each of them.

User Agent

Any device used to access a web page. A user agent might be a graphical browser, such as Internet Explorer or a web-enabled mobile phone.

Appendix

This appendix provides some sample files for your reference:

- MLSListings SAML Metadata
- Sample SAML <AuthnRequest>
- Sample SAML <Response>
- Sample SAML <Response> with Impersonation

The <AuthnRequest> and <Response> samples were generated with MLSListings acting in both the identity provider and service provider roles.

Actual copies of the files are available on the MLSListings Product Information page. (Home > Reference Library > Product Information > SSO Integration).

Important: Sample files are subject to change, contact MLSListings for the latest information.

MLSListings SAML Metadata

```
<md:EntityDescriptor xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  entityID="https://connect.staging.mlslistings.com/SAML/"
  cacheDuration="P7DT0H0M0S">
  <md:IDPSSODescriptor ID="AuthnRequestResponder"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    WantAuthnRequestsSigned="false">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>

            <ds:X509Certificate>MIIB+DCCAWWgAwIBAgIQFlD7lTTR6b1Pz
            W8CEfrqXDAJBgUrDgMCHQUAMCoxKDAmBgNVBAMTH2Nvbm5lY3Quc3
            RhZ2luZy5tbHNsaXN0aW5ncy5jb20wHhcNMDgxMDE1MTgxNDEwWhc
            NMTgxMDEzMTgxNDEwWjAqMSgwJgYDVQQDEx9jb25uZWN0LnN0YWdp
            bmcubWxzbGlzdGluZ3MuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNA
            DCBiQKBgQCajilkqzfELmMBrOBjbxFlyd8cI3FHjlhD1ULmUnoJ6x
            MuMaxI9hsGmB6ViSb5hGMAx1+4AG57Ajsd1OjXW5Av0Bpr/tgGrH2
            iCUD4Q3lkODhy069UBtAfu7gnwsM/U5ptFfWFtGVUYYwaFZP5nU2H
            3nNcEbq9tWD+J7TW1uDL8QIDAQABoycwJTATBgNVHSUEDDAKBggrB
            gEFBQcDATAOBgNVHQ8EBwMFALAAAAAwCQYFKw4DAh0FAAOBgQCP/f
            p5yDOs0BSysm9ml+He/StzuI1TEvovTcXqJaOdldWtIetq5cUIfN8
            PQ8kPjqXcC68C8eyfPK8WqDoYjXE/qBoFE68h5fPe/ktunIFWx1VJ
            tFP2MqAuA3q2v53xShET7MQPs2YNQOUkgmN7qAMyaPNQPy45xNupF
            iYG2Ec7dQ==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo>
        <ds:X509Data>

            <ds:X509Certificate>MIIB+DCCAWWgAwIBAgIQFlD7lTTR6b1Pz
            W8CEfrqXDAJBgUrDgMCHQUAMCoxKDAmBgNVBAMTH2Nvbm5lY3Quc3
            RhZ2luZy5tbHNsaXN0aW5ncy5jb20wHhcNMDgxMDE1MTgxNDEwWhc
            NMTgxMDEzMTgxNDEwWjAqMSgwJgYDVQQDEx9jb25uZWN0LnN0YWdp
            bmcubWxzbGlzdGluZ3MuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNA
            DCBiQKBgQCajilkqzfELmMBrOBjbxFlyd8cI3FHjlhD1ULmUnoJ6x
            MuMaxI9hsGmB6ViSb5hGMAx1+4AG57Ajsd1OjXW5Av0Bpr/tgGrH2
            iCUD4Q3lkODhy069UBtAfu7gnwsM/U5ptFfWFtGVUYYwaFZP5nU2H
            3nNcEbq9tWD+J7TW1uDL8QIDAQABoycwJTATBgNVHSUEDDAKBggrB
            gEFBQcDATAOBgNVHQ8EBwMFALAAAAAwCQYFKw4DAh0FAAOBgQCP/f
            p5yDOs0BSysm9ml+He/StzuI1TEvovTcXqJaOdldWtIetq5cUIfN8
            PQ8kPjqXcC68C8eyfPK8WqDoYjXE/qBoFE68h5fPe/ktunIFWx1VJ
            tFP2MqAuA3q2v53xShET7MQPs2YNQOUkgmN7qAMyaPNQPy45xNupF
            iYG2Ec7dQ==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://connect.staging.mlslistings.com/SAML/
      AuthnRequestResponder.ashx" />
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://connect.staging.mlslistings.com/SAML/
      AuthnRequestResponder.ashx" />
```

```
      <saml:Attribute Name="FullName"
        NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:unspecified" />
      <saml:Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:unspecified" />
      <saml:Attribute Name="MLSDomain"
        NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:unspecified" />
      <saml:Attribute Name="MLSMemberID"
        NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:unspecified" />
      <saml:Attribute Name="MemberOfficeRelationshipID"
        NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:unspecified" />
    </md:IDPSSODescriptor>
    <md:SPSSODescriptor AuthnRequestsSigned="false" ID="ACS"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
      WantAssertionsSigned="true">
      <md:AssertionConsumerService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" index="0"
        isDefault="true"
        Location="https://connect.staging.mlslistings.com/SAML/
        AssertionConsumerService.ashx" />
    </md:SPSSODescriptor>
    <md:Organization>
      <md:OrganizationName xml:lang="en">MLSListings
        Inc.</md:OrganizationName>
      <md:OrganizationDisplayName xml:lang="en">MLSListings
        Inc.</md:OrganizationDisplayName>
      <md:OrganizationURL
        xml:lang="en">http://www.mlslistings.com/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="administrative">
      <md:Company>MLSListings Inc.</md:Company>
      <md:GivenName>MLSListings</md:GivenName>
      <md:SurName>Receptionist</md:SurName>
      <md:EmailAddress>receptionist@mlslistings.com</md:EmailAddress>
      <md:TelephoneNumber>408-874-0200</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson contactType="billing">
      <md:Company>MLSListings Inc.</md:Company>
      <md:GivenName>Accounts</md:GivenName>
      <md:SurName>Payable</md:SurName>
      <md:EmailAddress>accountspayable@mlslistings.com</md:EmailAddress>
      <md:TelephoneNumber>408-874-0200</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson contactType="support">
      <md:Company>MLSListings Inc.</md:Company>
      <md:GivenName>Customer Service</md:GivenName>
      <md:SurName>Call Center</md:SurName>
      <md:EmailAddress>support@mlslistings.com</md:EmailAddress>
      <md:TelephoneNumber>866-734-5787</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson contactType="technical">
      <md:Company>MLSListings Inc.</md:Company>
      <md:GivenName>Joel</md:GivenName>
      <md:SurName>Allison</md:SurName>
      <md:EmailAddress>jallison@mlslistings.com</md:EmailAddress>
      <md:TelephoneNumber>408-874-0271</md:TelephoneNumber>
    </md:ContactPerson>
  </md:EntityDescriptor>
```

Sample SAML <AuthnRequest>

```
<samlp:AuthnRequest ID="_1914dbaa-e846-4d3b-83d1-dc06e18a2436" Version="2.0"
   IssueInstant="2010-02-09T21:39:32Z"
   Destination="https://connect.staging.mlslistings.com/SAML/AuthnRequestResponder.ashx"
   ForceAuthn="false" IsPassive="false"
   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   AssertionConsumerServiceIndex="0"
   AssertionConsumerServiceURL="https://connect.staging.mlslistings.com/SAML/
   AssertionConsumerService.ashx" AttributeConsumingServiceIndex="0"
   ProviderName="MLSListings" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<saml:Issuer
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://connect.staging.
   mlslistings.com/SAML/</saml:Issuer>
<samlp:NameIDPolicy AllowCreate="true" />
   </samlp:AuthnRequest>
```

Sample SAML <Response>

```
<samlp:Response ID="_dc33ac9b-0bca-43aa-9235-8db6274dc0f9" InResponseTo="
   _1914dbaa-e846-4d3b-83d1-dc06e18a2436" Version="2.0"
   IssueInstant="2010-02-09T21:39:43Z"
   Destination="https://connect.staging.mlslistings.com/SAML/AssertionConsumerService.
   ashx" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<saml:Issuer
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://connect.staging.
   mlslistings.com/SAML/</saml:Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#_dc33ac9b-0bca-43aa-9235-8db6274dc0f9">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces PrefixList="#default code ds kind rw saml samlp typens"
   xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" />
   </Transform>
   </Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>x4IBWCGUgIAjI66NVelVl7p++J0=</DigestValue>
   </Reference>
   </SignedInfo>

   <SignatureValue>aEYjUYJFsXYh2TagS6WbYJ65fdunJ2OwUiHiYrXr35uR6TArZ6P5rtWScDjbbdV6XoC6H
   refW22h5/fTQS/B6f9kUCL66Ir4FX3yVVqb7pvjksmV8jeIQxVQKvgakO8FPUdt/xLFVqVe+JNmmQ1ki3JAK3
   Zqq1X0p7WPkQ2AyhA=</SignatureValue>
<KeyInfo>
<X509Data>

   <X509Certificate>MIIB+DCCAWWgAwIBAgIQFlD7lTTR6b1PzW8CEfrqXDAJBgUrDgMCHQUAMCoxKDAmBgNV
   BAMTH2Nvbm5lY3Quc3RhZ2luZy5tbHNsaXN0aW5ncy5jb20wHhcNMDgxMDE1MTgxNDEwWhcNMTgxMDEzMTgxN
   DEwWjAqMSgwJgYDVQQDEx9jb25uZWN0LnN0YWdpbmcubWxzbGlzdGluZ3MuY29tMIGfMA0GCSqGSIb3DQEBAQ
   UAA4GNADCBiQKBgQCajilkqzfELmMBrOBjbxFlyd8cI3FHjlhD1ULmUnoJ6xMuMaxI9hsGmB6ViSb5hGMAx1+
   4AG57Ajsd1OjXW5Av0Bpr/tgGrH2iCUD4Q3lkODhy069UBtAfu7gnwsM/U5ptFfWFtGVUYYwaFZP5nU2H3nNc
   Ebq9tWD+J7TW1uDL8QIDAQABoycwJTATBgNVHSUEDDAKBggrBgEFBQcDATAOBgNVHQ8EBwMFALAAAAAwCQYFK
   w4DAh0FAAOBgQCP/fp5yDOs0BSysm9ml+He/StzuI1TEvovTcXqJaOdldWtIetq5cUIfN8PQ8kPjqXcC68C8e
   yfPK8WqDoYjXE/qBoFE68h5fPe/ktunIFWx1VJtFP2MqAuA3q2v53xShET7MQPs2YNQOUkgmN7qAMyaPNQPy4
   5xNupFiYG2Ec7dQ==</X509Certificate>
   </X509Data>
   </KeyInfo>
   </Signature>
```

```
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
<saml:Assertion Version="2.0" ID="_119735e2-6b9e-471d-b4d1-bdca57a7c045"
   IssueInstant="2010-02-09T21:39:43Z"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Issuer>https://connect.staging.mlslistings.com/SAML/</saml:Issuer>
<saml:Subject>
<saml:NameID>81234040</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2010-02-09T22:39:43Z"
   Recipient="https://connect.staging.mlslistings.com/SAML/"
   InResponseTo="_1914dbaa-e846-4d3b-83d1-dc06e18a2436" />
  </saml:SubjectConfirmation>
  </saml:Subject>
<saml:Conditions NotBefore="2010-02-09T21:39:43Z" NotOnOrAfter="2010-02-09T22:39:43Z">
<saml:AudienceRestriction>
<saml:Audience>https://connect.staging.mlslistings.com/SAML/</saml:Audience>
  </saml:AudienceRestriction>
  </saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-02-09T21:39:43Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
  </saml:AuthnContextClassRef>
  </saml:AuthnContext>
  </saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="FullName" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>Carol Martin</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>cmartin@mlslistings.com</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="MLSDomain" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>MLSListings</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="MLSMemberID" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>81234040</saml:AttributeValue>
  </saml:Attribute>
<saml:Attribute Name="EffectiveSubject"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>81234040</saml:AttributeValue>
  </saml:Attribute>
  </saml:AttributeStatement>
  </saml:Assertion>
  </samlp:Response>
```

Sample SAML <Response> with Impersonation

```
<samlp:Response ID="_ada61669-8d53-4abb-988e-24629d430a04" InResponseTo="
   _9eb9f4df-bcda-4695-8e2b-dc86e69a2280" Version="2.0"
   IssueInstant="2010-02-09T21:48:55Z"
   Destination="https://connect.staging.mlslistings.com/SAML/AssertionConsumerService.
   ashx" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<saml:Issuer
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://connect.staging.
   mlslistings.com/SAML/</saml:Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
```

```
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#_ada61669-8d53-4abb-988e-24629d430a04">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces PrefixList="#default code ds kind rw saml samlp typens"
   xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" />
   </Transform>
   </Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>A674scEHSTleubGdl6cf0hB2iwo=</DigestValue>
   </Reference>
   </SignedInfo>

   <SignatureValue>OInGpzjyu8/8qOL1sLOSlNa9p1O0ss/AQr5DZQVkXQa9jwdjd9Zzu+XsSJI2GodN/1pS0
   e/6ZBPvjzg5qMCmb607lyy0WXKIWQDiU9gOSJ63njAx7iU01K3m55uccKWYjyaLSo7uhLoyQeC1rtMjk2Wxs0
   5FSWz6XgDYntAAsbI=</SignatureValue>
<KeyInfo>
<X509Data>

   <X509Certificate>MIIB+DCCAWWgAwIBAgIQFlD7lTTR6b1PzW8CEfrqXDAJBgUrDgMCHQUAMCoxKDAmBgNV
   BAMTH2Nvbm5lY3Quc3RhZ2luZy5tbHNsaXN0aW5ncy5jb20wHhcNMDgxMDE1MTgxNDEwWhcNMTgxMDEzMTgxN
   DEwWjAqMSgwJgYDVQQDEx9jb25uZWN0LnN0YWdpbmcubWxzbGlzdGluZ3MuY29tMIGfMA0GCSqGSIb3DQEBAQ
   UAA4GNADCBiQKBgQCajilkqzfELmMBrOBjbxFlyd8cI3FHjlhD1ULmUnoJ6xMuMaxI9hsGmB6ViSb5hGMAx1+
   4AG57Ajsd1OjXW5Av0Bpr/tgGrH2iCUD4Q3lkODhy069UBtAfu7gnwsM/U5ptFfWFtGVUYYwaFZP5nU2H3nNc
   Ebq9tWD+J7TW1uDL8QIDAQABoycwJTATBgNVHSUEDDAKBggrBgEFBQcDATAOBgNVHQ8EBwMFALAAAAAwCQYFK
   w4DAh0FAAOBgQCP/fp5yDOs0BSysm9ml+He/StzuI1TEvovTcXqJaOdldWtIetq5cUIfN8PQ8kPjqXcC68C8e
   yfPK8WqDoYjXE/qBoFE68h5fPe/ktunIFWx1VJtFP2MqAuA3q2v53xShET7MQPs2YNQOUkgmN7qAMyaPNQPy4
   5xNupFiYG2Ec7dQ==</X509Certificate>
   </X509Data>
   </KeyInfo>
   </Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
<saml:Assertion Version="2.0" ID="_0dbbc13f-c1fb-47e0-9f93-726fc5341cb2"
   IssueInstant="2010-02-09T21:48:55Z"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Issuer>https://connect.staging.mlslistings.com/SAML/</saml:Issuer>
<saml:Subject>
<saml:NameID>81234040</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2010-02-09T22:48:55Z"
   Recipient="https://connect.staging.mlslistings.com/SAML/" InResponseTo="
   _9eb9f4df-bcda-4695-8e2b-dc86e69a2280" />
   </saml:SubjectConfirmation>
   </saml:Subject>
<saml:Conditions NotBefore="2010-02-09T21:48:55Z" NotOnOrAfter="2010-02-09T22:48:55Z">
<saml:AudienceRestriction>
<saml:Audience>https://connect.staging.mlslistings.com/SAML/</saml:Audience>
   </saml:AudienceRestriction>
   </saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-02-09T21:48:55Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
   </saml:AuthnContextClassRef>
   </saml:AuthnContext>
   </saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="FullName" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>Carol Martin</saml:AttributeValue>
   </saml:Attribute>
```

```
<saml:Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>cmartin@mlslistings.com</saml:AttributeValue>
   </saml:Attribute>
<saml:Attribute Name="MLSDomain" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>MLSListings</saml:AttributeValue>
   </saml:Attribute>
<saml:Attribute Name="MLSMemberID" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>81234040</saml:AttributeValue>
   </saml:Attribute>
<saml:Attribute Name="EffectiveSubject"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>81234020</saml:AttributeValue>
   </saml:Attribute>
<saml:Attribute Name="EffectiveFullName"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>Jim Harrison</saml:AttributeValue>
   </saml:Attribute>
<saml:Attribute Name="EffectiveEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:
   attrname-format:basic">
<saml:AttributeValue>jharrison@mlslistings.com</saml:AttributeValue>
   </saml:Attribute>
   </saml:AttributeStatement>
   </saml:Assertion>
   </samlp:Response>


     <samlp:Response ID="_dc33ac9b-0bca-43aa-9235-8db6274dc0f9"
        InResponseTo="_1914dbaa-e846-4d3b-83d1-dc06e18a2436
```