Single Sign On (SSO) and B2B Contract Enquiry

28 September 2016

V2.0

Implementation Support Guide

Contents

Introduction

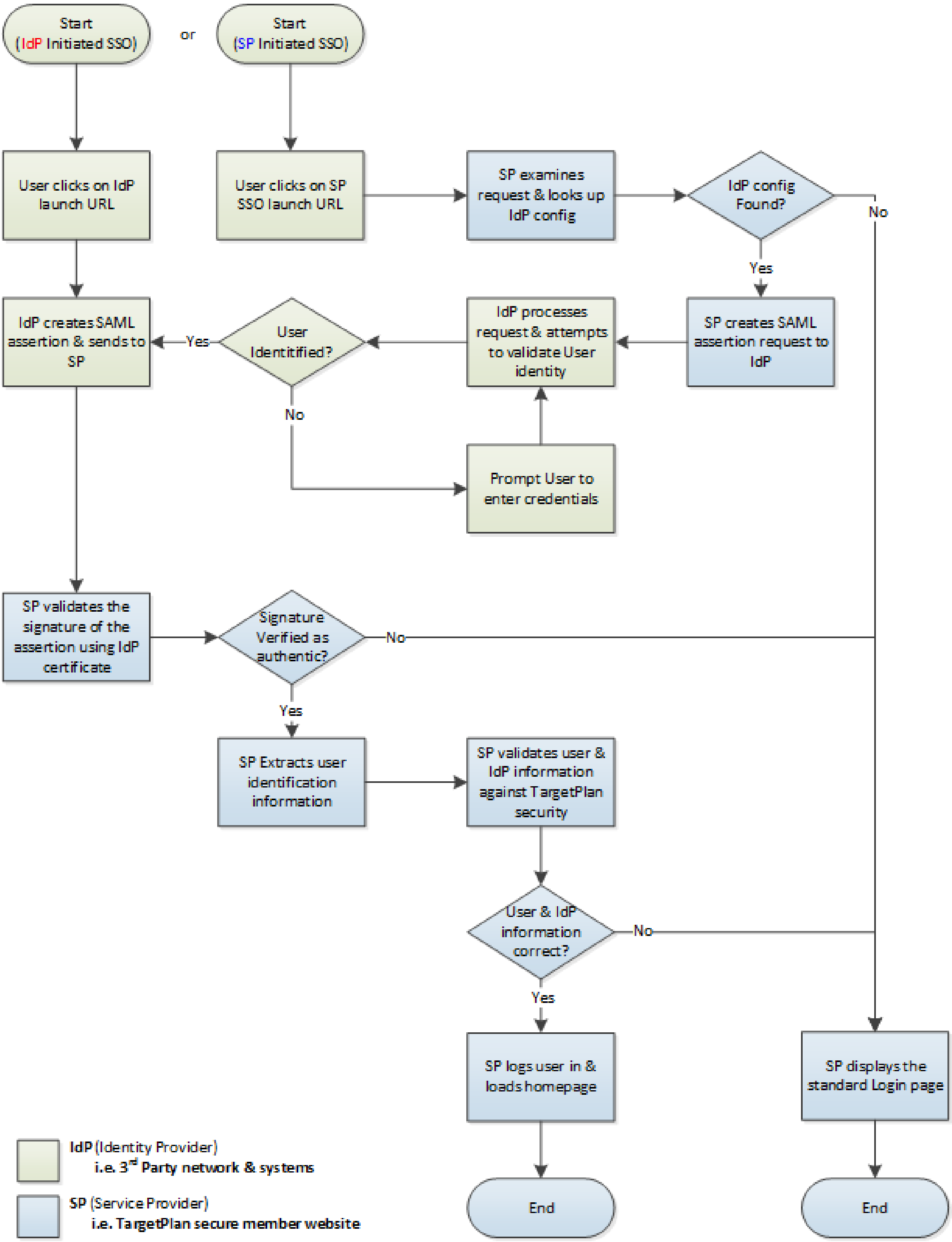
This document describes how single sign on (SSO) can be implemented to enable members currently authenticated in third-party systems to access TargetPlan, our secure member website, without the need to enter a username and password.

This streamlined process supports OASIS Security Assertion Markup Language (SAML) 2.0 standard and relies upon a third-party performing the necessary authentication on their own internal systems to prevent unauthorised access. This process works by the third-party confirming that the authenticating user is valid and trusted. TargetPlan SSO supports Identity Provider (IdP) Initiated SSO and Service Provider (SP) Initiated SSO.

This document describes the TargetPlan SSO functionality, deep linking functionality and member enquiry services available. This document should be read in conjunction with the OASIS SAML standards (*see: Additional Information & References P.15*) and does not attempt to repeat all information contained in the standards.

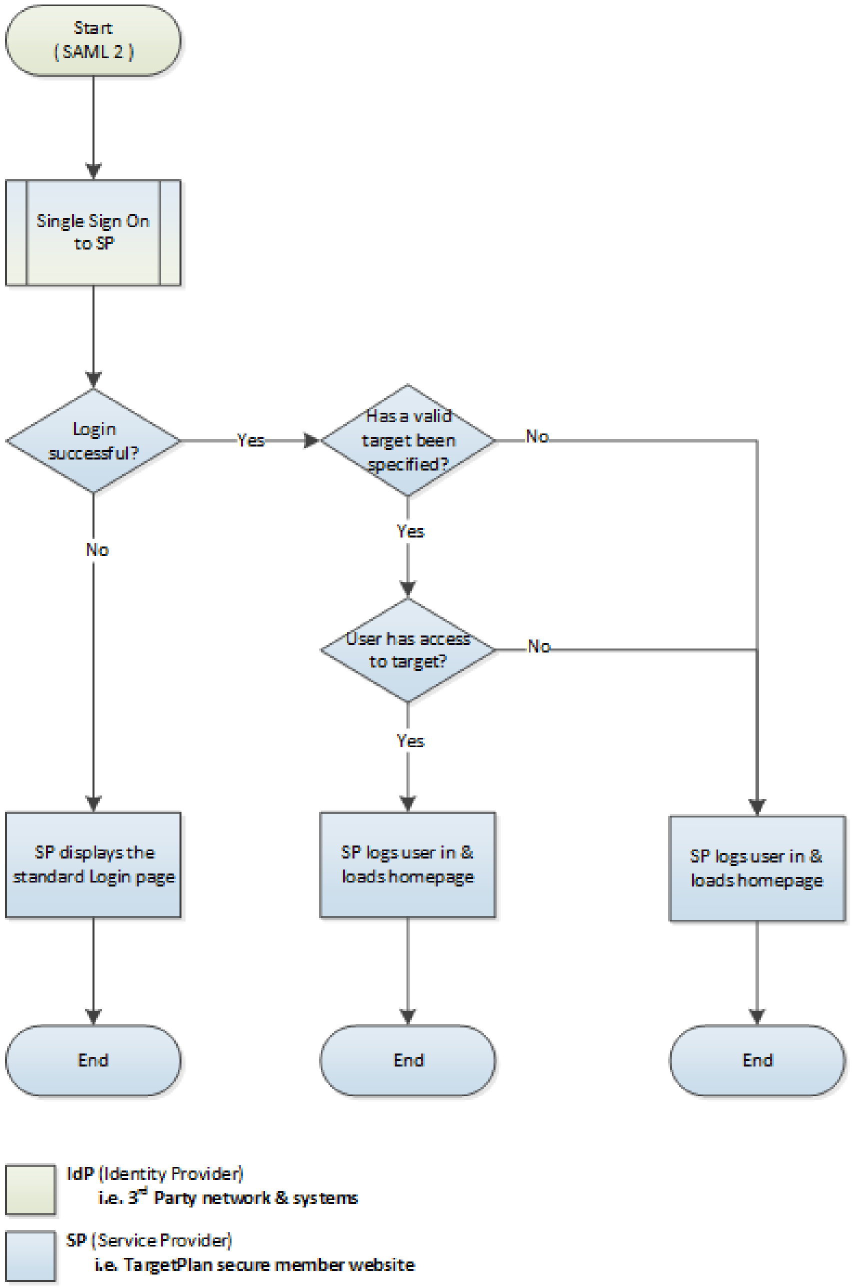
High Level Process - SSO

The following diagram represents how TargetPlan SSO allows members to seamlessly log on without asking for username and password credentials. The diagram includes both IdP initiated and SP initiated SSO.


Start (IdP Initiated SSO)
or
Start (SP Initiated SSO)
User clicks on IdP launch URL
User clicks on SP SSO launch URL
SP examines request & looks up IdP config
IdP config Found?
No
Yes
IdP creates SAML assertion & sends to SP
Yes
User Identitified?
IdP processes request & attempts to validate User identity
SP creates SAML assertion request to IdP
No
Prompt User to enter credentials
SP validates the signature of the assertion using IdP certificate
Signature Verified as authentic?
No
Yes
SP Extracts user identification information
SP validates user & IdP information against TargetPlan security
User & IdP information correct?
No
Yes
SP logs user in & loads homepage
SP displays the standard Login page
End
End
IdP (Identity Provider)
i.e. 3rd Party network & systems
SP (Service Provider)
i.e. TargetPlan secure member website

High Level Process – SSO Deep Linking (RelayState)

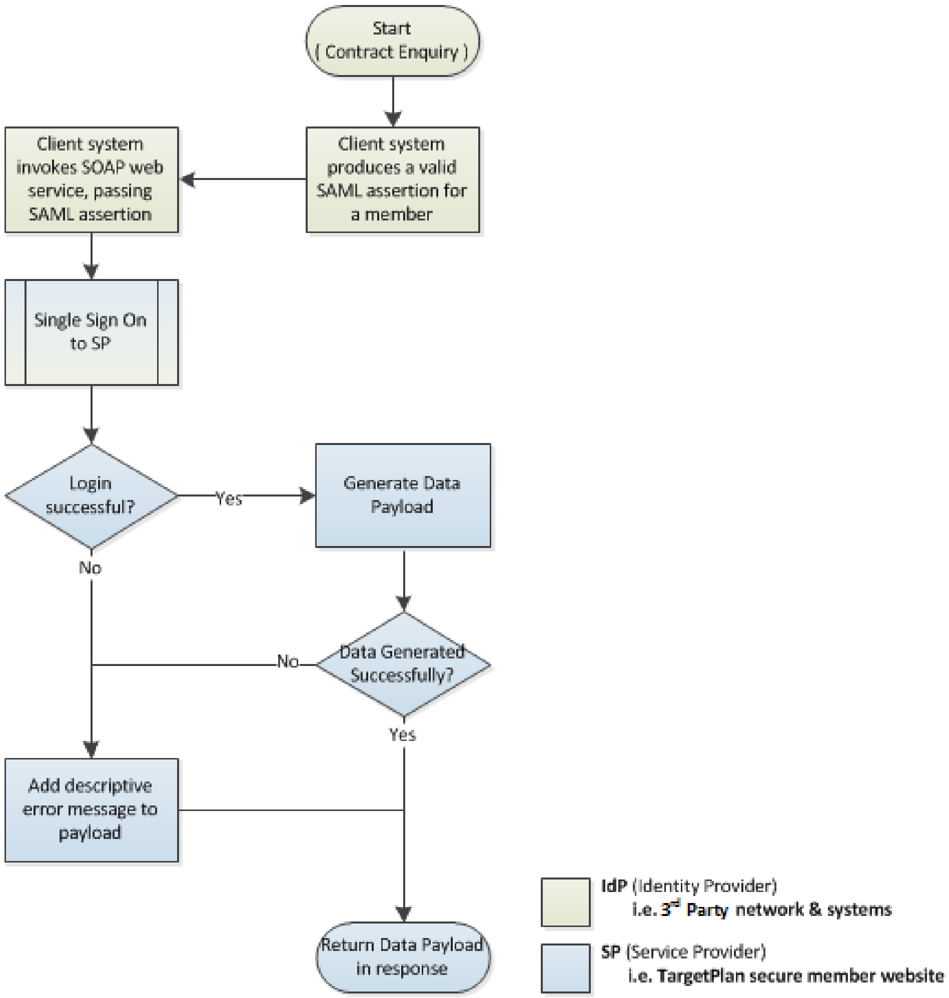
TargetPlan has a feature to allow an identity provider to define a specific page to show after SSO launch, instead of the homepage. This might be used, for instance, to take members directly to the change contribution screen during a flex enrolment window. The following diagram is a high-level process flow of how this works:


Start
(SAML 2)
Single Sign On to SP
Login successful?
Yes
No
Has a valid target been specified?
No
Yes
User has access to target?
No
Yes
SP displays the standard Login page
SP logs user in & loads homepage
SP logs user in & loads homepage
End
End
End
IdP (Identity Provider)
i.e. 3rd Party network & systems
SP (Service Provider)
i.e. TargetPlan secure member website

High Level Process – Member Enquiry Services

In addition to the secure member website elements, TargetPlan also provides web services that can be used to query member pension information programmatically. They can be invoked by submitting a SOAP message containing a valid SAML assertion.

This feature can be used to present a member’s pension information directly on a third-party site, for instance, adding a section to a flex benefit system to show the logged in member’s fund allocation or contribution directly, in addition to the SSO launch of TargetPlan.


Start
(Contract Enquiry)
Client system produces a valid SAML assertion for a member
Client system invokes SOAP web service, passing SAML assertion
Single Sign On to SP
Login successful?
Yes
No
Generate Data Payload
Data Generated Successfully?
No
Yes
Add descriptive error message to payload
Return Data Payload in response
IdP (Identity Provider)
i.e. 3rd Party network & systems
SP (Service Provider)
i.e. TargetPlan secure member website

The SOAP Web services available are as follows:

Member Information Service

This service accepts a valid SAML assertion and responds with a condensed member account in a single structure that includes:

- Scheme
- Account Information
- Target Retirement Age
- Contributions (level of contribution(s) & investment strategy*)
- Investments (the fund holdings* and values of the pension account)
- Income & disinvestment strategy* (for drawdown schemes)

Member Account Statement

This service accepts a valid SAML assertion plus a date range and responds with a condensed member account in a single structure that includes:

- Summary Information (opening & closing balances)
- Transactional Information (contributions*, switches*, etc)

**

**Note - All funds are expressed down to index level for modelling purposes. For instance, if a member currently has a holding in a freestyle fund, then that freestyle fund will also be expressed proportionally in terms of known indices.*

Implementation

Initial Engagement

The first steps for configuring SSO between a third-party and TargetPlan will consist of the following:

- Decide upon the type of SSO (IdP or SP initiated SSO).

- Decide upon the member identifier to use. TargetPlan currently supports three types of identifier:
  - TargetPlan account number (A/000123456)
  - National Insurance Number (QQ123456A)
  - Email Address (member.name@client.com)

- Decide upon the environment to prove out. Aegon can support SSO in a dedicated test environment first, or in production*.

- Client to provide their SAML metadata (including message validation 509 certificate).

*Note that Aegon would always expect implementations using member enquiry web services to use the test environment in the first instance.

Setup Proving

Once Aegon have received the information above, the SSO configuration can be added to the required environment by the TargetPlan implementation team.

To confirm connectivity, the implementation team will issue an account to use for testing. TargetPlan supports demo user functionality in all environments - any valid and correctly configured IdP issued assertion should be able to launch any demo user. This is particularly useful for setting up SSO ahead of a new scheme take-on, since it does not require a scheme to be fully set-up and working. If the third-party already has a demo account, the SSO can be configured to launch this user. Demo capability is also supported within the member enquiry web services. Once this is complete, the tests can then be performed on a “real” member in test*, or production as appropriate.

* Note that Aegon have a suite of logging tools available in the test environment to support configuration proving of SSO and member enquiry SOAP web services. Technology teams are on hand during this process to support the implementation as appropriate.

Technical Details

URLs

TargetPlan SSO

Item	URL
Test	https://lwp.test.aegon.co.uk/targetplan/SAML2POST.do
Prod	https://www.aegon.co.uk/targetplan/SAML2POST.do

TargetPlan (where users will be directed to after authentication, successful or otherwise)

Item	URL
Test	https:// lwp.test.aegon.co.uk/targetplan
Prod	https://www.aegon.co.uk/targetplan

Member Information Service

Item	URL
Test	https://lwp.test.aegon.co.uk/targetplan/services/MemberInformationService.wsdl
Prod	https://lwp.aegon.co.uk/targetplan/services/MemberInformationService.wsdl

Member Transaction Service

Item	URL
Test	https:// lwp.test.aegon.co.uk/targetplan/services/MemberAccStatementService.wsdl
Prod	https://lwp.aegon.co.uk/targetplan/services/MemberAccStatementService.wsdl

Note that URLs for application & page names should be considered case sensitive, and the above case should be used.

SAML Configuration Details

Element	Value
SAML Standard	All data elements in the SAML exchange should adhere to OASIS SAML2.0 standard.
Token Name	SAMLResponse
Name ID Format	Entity
SAML Binding	The SAML HTTP Post binding will be used for IdP initiated SSO.
Audience Condition	(prod) https://lwp.aegon.co.uk/targetplan (test) https://lwp.test.aegon.co.uk/targetplan
Assertion Duration Condition	NotBefore & NotOnOrAfter conditions should be configured with a duration to allow for the possibility of different system clocks. Recommendation is for 2 mins before & after IdP time (4min duration). Timezone notation ("Z" for UTC) should be included for all times.
Subject Confirmation	Bearer
SAML attribute	The following attributes are acceptable: 1. **nameid** (value can be *any* of the below) 2. **email** (and email address registered to the individual on the AWS platform) 3. **accountno** (pension account number) 4. **nino** (national insurance number) *Notes* ** TargetPlan will ignore any attributes not named exactly as stated above (for example: ClientId).* ** If more than one attribute is supplied that matches the above list, the order in the list above takes precedence (for example if a nameid & nino are provided, the nameid will be used).* ** Format of 1,3 & 4 should adhere to:* ***"urn:oasis:names:tc:SAML:2.0:nameid-format:string"*** ** Format of 2 should adhere to:* ***"urn:oasis:names:tc:SAML:2.0:attrname-format:uri"***

SAML Security

- The TargetPlan system does not currently support encryption of SAML assertions or attributes with an Aegon specific public key (assertions are always validated against the IdP keys however).
- One Time Use assertion rules are not enforced at SP level.
- Uniqueness of Request ID's are not enforced at SP level.
- Validity length of assertion is not enforced.
- TargetPlan has a session inactivity timeout of 10 mins.
- In the event of any kind of failure in the SAML validation or SSO login process, the end user will be redirected to the TargetPlan login page (where an end user can login directly, reset their password or register for access, if applicable).
- RelayState is applied in accordance with SAML standards, with the following parameters configured:

Relay State Parameters

Item	Description
home	Homepage dashboard is shown (default).
statement	Loads the pension statement screen where an online statement can be produced based upon different date ranges.
fundinfo	Loads the fund information and comparison screen.
summary	Loads the current pension account summary screen.
investment	Loads the investments screen where current fund allocations & future elections can be viewed and changed.
contribution	Loads the contribution screen in read mode.
changecontribution	Loads the contribution screen directly into the edit mode of the screen with the values ready to be changed (if the member permissions allow edit at the time of the launch – if not, the view screen is shown instead).
message	Loads the message centre dashboard (if applicable for scheme).
contact	Loads the contact us page.

Frequently Asked Questions

Q. Members of my scheme need to be able to SSO into TargetPlan from my company intranet and a separate benefit consultant website too. Is this possible?

A. Yes – We can configure more than one IdP against a single scheme or schemes.

Q. My company is responsible for members in more than one scheme in TargetPlan. Will this work?

A. Yes – We can configure the same IdP against multiple schemes

Q. If we setup SSO, does this stop members logging in directly with their username/passwords?

A. No – SSO is an additional feature & does not replace the normal login.

Q. How long does this setup process usually take?

A. This is pure configuration by our implementation team, so turnaround time is typically within a week or two, once the details have been provided.

Q. My scheme is still in the process of being on-boarded. Can I see SSO working before then?

A. Yes – if IdP information is available then it's possible to configure SSO to use a demo account up front in either TEST or Production.

Q. What if it doesn't work first time?

A. While it's possible it might not work first time, the Aegon test environment has full tracing capability and the technology teams are on hand to investigate root causes and identify the solution. Typical causes of this are down to the name of the entity attribute or the x509 signed assertion certificate being different in each environment.

Q. I am interested in using the B2B contract enquiry services. Do you have any more in depth information for my developers?

A. We can work with your development teams. Contact your Client Relationship Manager for more information.

Additional Information & References

OASIS SAML

- SAML Standard: http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

- SAML Overview: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

OpenSAML

- Opensaml is open source libraries for working with SAML in java.
- It contains simple implementation of all xml handling procedures, that can be easily incorporated with
- Opensaml library providers easy way to handle xml document and decoding, unmarshaling, validating certificate, extracting attributes from xml objects, validating SAML response, verifying other security aspects such as timestamp.

SAML references

- OpenSAMl libraries: https://wiki.shibboleth.net/confluence/display/OpenSAML/Home

- OpenSAMl for Java : https://wiki.shibboleth.net/confluence/display/OpenSAML/OSTwoDeveloperManual

Example SAML2.0 POST Message

This is a sample of Base64 Decoded SAML response from IDP that contains user id passed in an attribute statement (highlighted):

```
<saml2:Assertion ID="_3f31e515a127f0ddc4b1be6c"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">IdP Issuer
</saml2:Issuer>
<saml2:Subject>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData Address="45.3.96.227" NotOnOrAfter="2014-03-
24T13:53:31.660Z" Recipient="https://sample.idp.com/webApp/SAML2POST.do"/>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2014-03-24T13:48:31.660Z" NotOnOrAfter="2014-03-
24T13:53:31.660Z">
<saml2:AudienceRestriction><saml2:Audience>https://sample.idp.com/webApp
</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2014-03-24T13:48:31.625Z">
<saml2:SubjectLocality Address="45.3.96.227"/>
<saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute FriendlyName="email" Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
userid@sample.com
</saml2:AttributeValue>
</saml2:Attribute></saml2:AttributeStatement>
</saml2:Assertion>
</saml2p:Response>
```

We're proud to be the
Lead Partner of British Tennis.