AIRnID© SAML Integration Overview

Introduction

This document is intended to give an overview of SAML and how it is leveraged by AIRnID to provide federated authentication across the web.

Purpose and Audience

This document is intended for technical personnel responsible for implementing AIRnID as an authentication mechanism for websites, applications, networks, etc. It is a high-level overview as the details of integration (such as shared attributes) should be discussed with NimbusID® technical staff on a case-by-case basis. It also provides a URL to AIRnID's SAML Metadata file.

SAML Assertions Overview

This section below is from the legacy SAML XML.org website at http://saml.xml.org/assertions. Current information on the SAML 2.0 standard can be reviewed at https://wiki.oasis-open.org/security/FrontPage.

An assertion consists of one or more statements. For SSO, a typical SAML assertion will contain a single authentication statement and possibly a single attribute statement. However, a SAML response could contain multiple assertions.

The outer structure of an assertion is generic, providing information common to all statements within it. The specific details in an assertion are contained in a series of inner elements describing the authentication, attribute, authorization decision, or user defined statements.

SAML is defined in terms of assertions, protocols, bindings and profiles.

An assertion is a package of information that supplies one or more statements made by a SAML Service Provider. SAML defines three different kinds of assertion statement that can be created by a SAML Service Provider:

Authentication

The subject was authenticated by a particular means at a particular moment in time. This kind of statement is typically generated by a SAML authority called an Identity Provider.

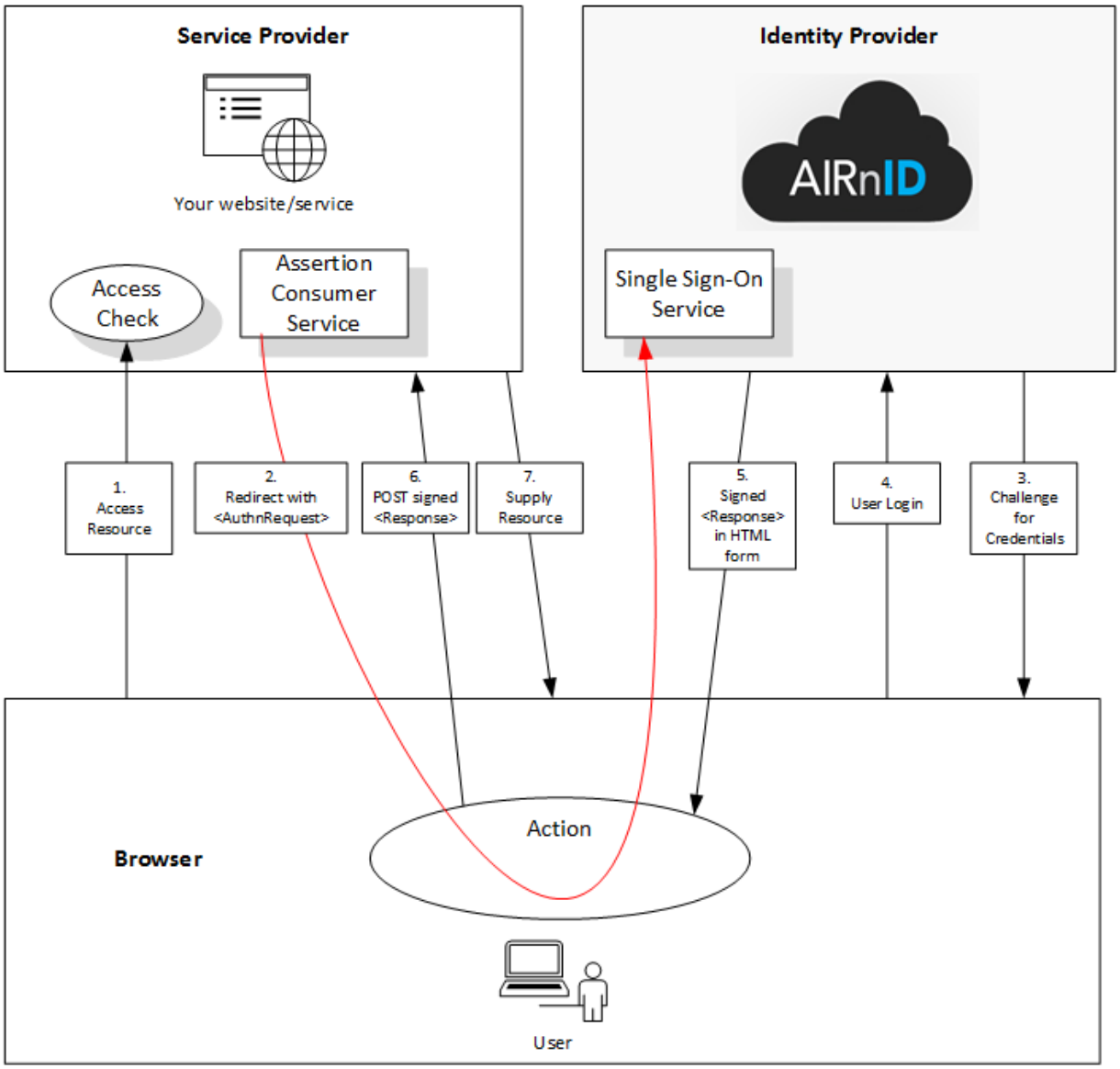
Attribute

The subject associated with the supplied attributes.

Authorization decision

Access to the resource was granted or denied.

SAML Flow with AIRnID



1. A user accesses their account to a service provider with a web browser or client application.
2. The service provider knows if the user is logged in or not. If not, a redirect to AIRnID is made with a *AuthnRequest* SAML token.
3. AIRnID receives the token, checks if the account is already logged. If not, the user is redirected to AIRnID's login page.
4. The user logs in with AIR authentication.
5. A signed Response in HTML form is sent from AIRnID to the user verifying the identity of the user.
6. A POST request is made of the signed response from the user to the SP.
7. Once validated, the user is allowed to access the service provider.

Identifying the User

Association of the AIRnID user with the user account in the SP's internal identity store is accomplished via custom SAML Attributes. These will vary depending on the type of identity store being utilized by the SP. For example, the SID attribute is recommended for Active Directory installations. NimbusID will work with the integrating party to assist in determining and making recommendations for the appropriate attribute to be used based on the integrating party's environment.

Requirements (Service Provider)

- SAML 2.0 support

AIRnID SAML Metadata File

https://auth.nimbusid.com/saml2/idp/metadata.php