Deployment Guide for Proxying Assurance between OpenID and SAML

Version: 0.8

Date: 2010-05-10

Editor: Paul Madsen, NTT

Tatsuki Sakushima, NRI

Contributors:

This document is a draft and not in final release form. The full list of contributors will be added prior to the final release of this document.

Status: This document is a draft Kantara Initiative Report, approved by the Concordia DG (see section 3.9 and 4 of the Kantara Initiative Operating Procedures).

Abstract: SAML and OpenID are key federated identity protocols. Both SAML and OpenID define mechanisms in support of expressing assurance information on protocol messages, respectively Authentication Context and the Provider Authentication Policy Extension (PAPE). In deployment scenarios that require proxying from one of the protocols to the other, it becomes necessary to map to and from the corresponding assurance mechanisms. This document provides guidance on this mapping and related issues.

Filename: Kantara-concordiadg-proxyingassurance-report-08.doc

Notice:

Contents

1 INTRODUCTION

In the context of federated identity protocols, assurance refers to the degree of confidence a Relying Party (RP) can ascribe to the identity assertions an Identity Provider (IdP) makes regarding end-users. In the absence of legal contracts indemnifying the RP from any risk involved in accepting such assertions, an RP's confidence (and consequent willingness to accept the assertions) may be increased through knowledge of the policies & processes followed by the IdP in issuing the assertion. For instance, in a Single Sign On application, the degree of confidence the RP has in the assertion from the IdP as to the authentication status of the User may depend on a number of factors, including how the User was originally registered at the IDP, and how they were subsequently authenticated.

Notwithstanding that assurance is ultimately a continuum, it is typically categorized into levels (LOA) for practicality. Assurance frameworks (such as NIST 800 63) stipulate the required policies and procedures that an IdP must perform in order to meet defined LOA.

Both SAML OpenID define mechanisms in support of expressing assurance information on protocol messages, respectively Authentication Context and the Provider Authentication Policy Extension (PAPE). Through these mechanisms, an RP is able to express its assurance expectations on its request message to the IdP for authentication, and the IdP is able to express the actual assurance achieved on its response message back.

In deployment scenarios that require proxying from one of the protocols to the other, it may become necessary for the proxying entity to map between the SAML and OpenID assurance mechanisms. While similar, the two mechanisms make different assumptions about expressing assurance - thereby creating the possibility of issues for the proxy. This document provides guidance to those entities playing the role of proxy on this mapping and related issues.

1.1 SAML Authentication Context

SAML Authentication Context [SAMLAC] provides a number of related mechanisms by which the SAML IDP & SP can indicate the nature of authentication, registration, proofing etc and thereby facilitate the RP establishing an appropriate level of assurance in the IDP's assertions. Authentication context is defined as the information, additional to the authentication assertion itself, that the relying party may require before it makes an entitlements decision with respect to an authentication assertion.

SAML defines authentication context classes to facilitate SPs making assurance decisions. Each class defines a proper subset of the full set of authentication contexts. Classes have been chosen as representative of the current practices and technologies for registration and authentication technologies.

The SAML LOA profile [SAMLLOA] defines how to bind levels of assurance to the existing SAML authentication context mechanism, as well as allowing a SAML IdP to advertise the levels of assurance it has been certified as being able to support.

1.2 OpenID Provider Authentication Policy Extension (PAPE)

The OpenID Provider Authentication Policy Extension (PAPE) [PAPE] allows the RP and OP to discuss the specifics of how the user authenticated to the OP. Through PAPE, an OpenID RP is able to add to the OpenID Authentication request additional authentication requirements, specifically stipulating its preference for how the user was authenticated, and specify how long ago that authentication is allowed to have occurred.

PAPE defines 3 URIs for what are expected to be relevant authentication mechanisms.

- http://schemas.openid.net/pape/policies/2007/06/phishing-resistant - An authentication mechanism where the End User does not provide a shared secret to a party potentially under the control of the Relying Party.
- http://schemas.openid.net/pape/policies/2007/06/multi-factor - an authentication mechanism where the End User authenticates to the OpenID Provider by providing over one authentication factor.
- http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical - An authentication mechanism where the End User authenticates to the OpenID Provider by providing over one authentication factor where at least one of the factors is a physical factor such as a hardware device or biometric.

In addition to specifying particular authentication technologies or characteristics, PAPE also supports more abstract LOA.

1.2.1 ICAM

The US government's Identity, Credential Access MAnagement (ICAM) Program has defined a profile for the use of OpenID 2.0 by US government departments [ICAMOpenID].

Amongst other aspects of OpenID, the ICAM profile stipulates how the PAPE parameter is to be used. Most notable is that the profile overrides PAPE's own distinction between authentication policy and assurance levels. The ICAM profile stipulates that the RP should specify assurance level identifiers in the PAPE 'openid.pape.preferred_auth_policies' parameter rather than use PAPE's LOA parameters.

The ICAM profile's use of PAPE's 'preferred_auth_policies' parameter to carry LOA sets a useful precedent, effectively mitigating the restriction inherent in PAPE's lack of support for specifying a particular LOA policy on a request. This guideline will follow this precedent.

2 MOTIVATION

For SSO, both SAML and OpenID depend on an interaction between a RP and an IdP - the RP requests of the IdP that a visiting User be authenticated and the fact and nature of this authentication be returned to the RP. Neither SAML nor OpenID require that the IdP actually itself perform the authentication - in principle allowing the IdP to outsource the job just like the RP did.

Consequently, it is possible for an authentication request sent from an OpenID RP to an OpenID Provider (OP) to be proxied by that OP using SAML to a SAML IdP for the actual authentication of the User through presentation of a credential. This might be the case if the original OpenID RP were to request a higher LOA than could be satisfied by the OP which, in order to satisfy the request, would proxy the request through SAML to a SAML IdP that could satisfy the desired LOA.

Some European National Research and Education Networks (NREN) are exploring this use case, i.e. bridging their SAML-based federations with OpenID.

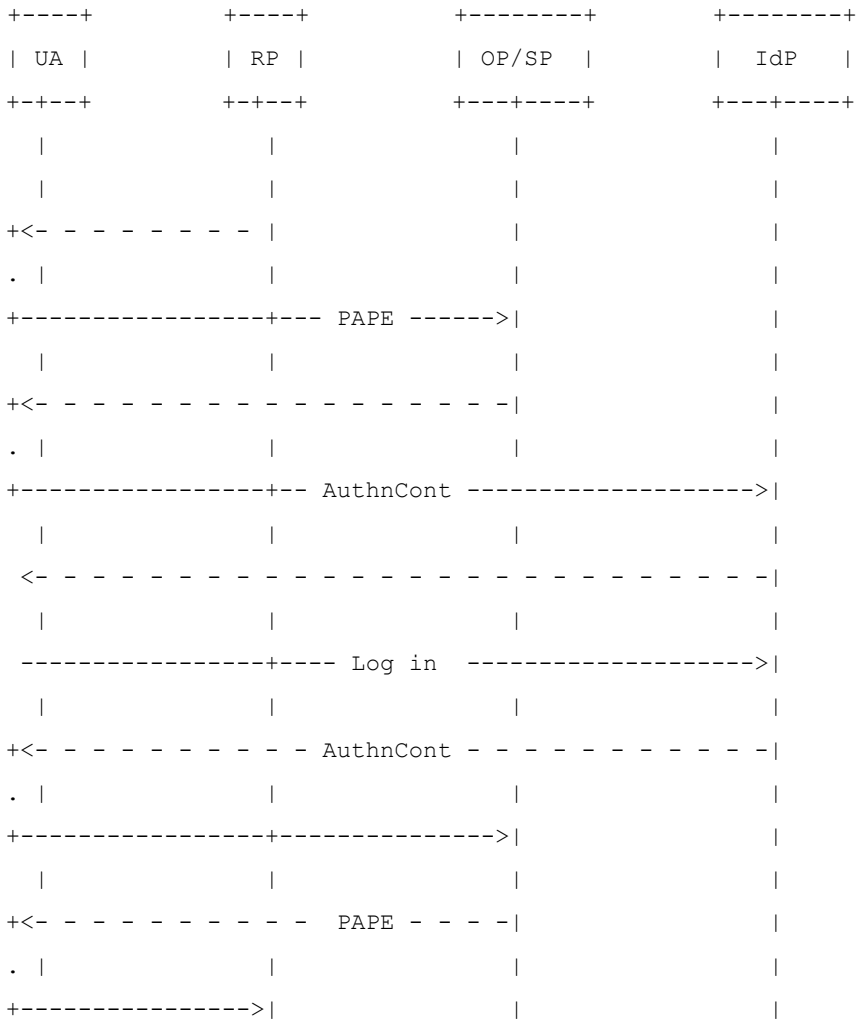
Likewise, it is possible for an authentication request sent from a SAML SP to an SAML IDP to be proxied by that IdP using OpenID to a OP for the actual authentication of the User. This might be the case if the original SAML SP were to request a lower LOA than than supported by the SAML IdP which, in order to satisfy the request, would proxy the request through OpenID to an OP that could satisfy the desired LOA.

3 SCENARIOS

There are two scenarios to consider, differentiated by the 'starting' protocol, ie that used by the site the user firsts interact with.

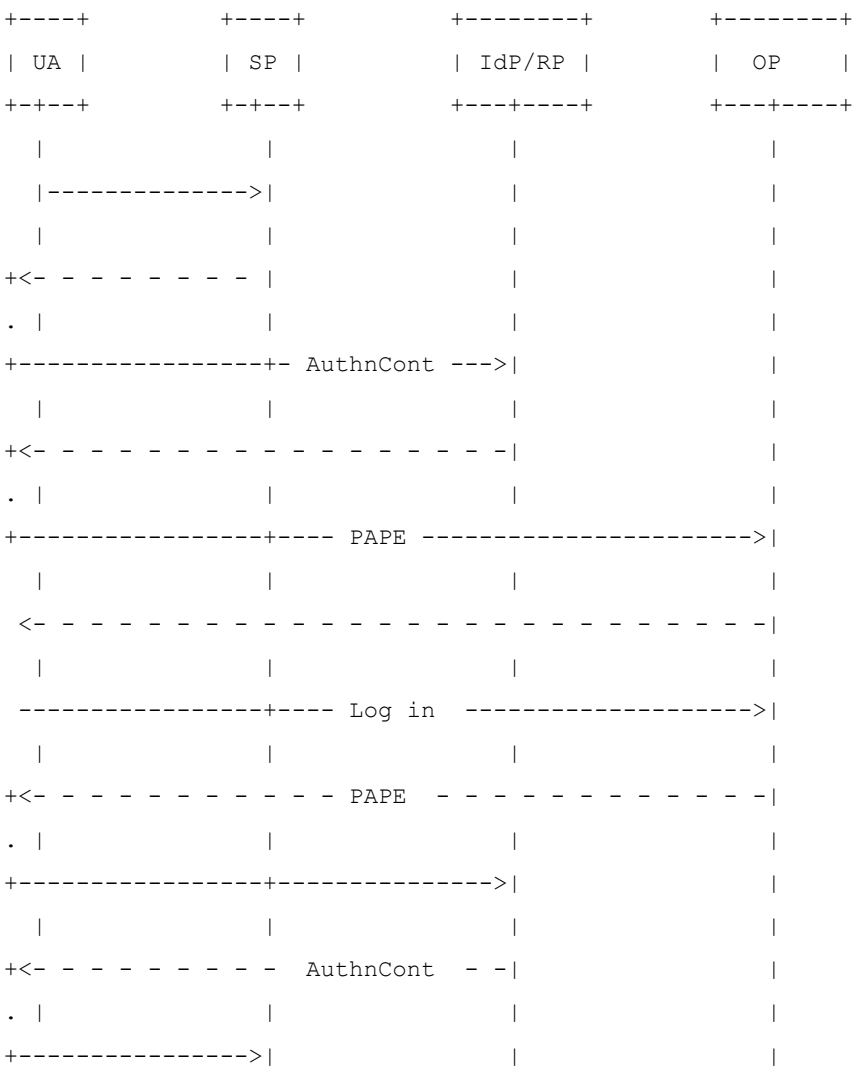
3.1 User visits OpenID RP

This scenario has the user visit an OpenID RP first. The authentication at the chosen OP is proxied through SAML to an appropriate IdP. This scenario is shown below:



3.2 User visits SAML SP

This scenario has the user visit a SAML SP first. The authentication at the chosen IdP is proxied through OpenID to an appropriate OP. This scenario is shown below


UA
SP
IdP/RP
OP
AuthnCont
PAPE
Log in
PAPE
AuthnCont

4 PROXYING GUIDELINES

Below are recommendations for the entity playing the role of protocol proxy between SAML & OpenID, differentiated by the protocol supported by the eventual consumer of the assertion.

4.1 User visits OpenID RP

4.1.1 Request

If the OpenID authentication request contains a PAPE policy URI that the OP is unable to satisfy, the OP MAY choose to proxy the request through SAML to an IdP that can.

If the OpenID authentication request has openid.mode = "checkid_immediate", the OP MUST specify ForceAuthn = "false" and isPassive = "true" on any proxied SAML Authentication request.

If proxying, the OP SHOULD give the User the ability to choose the SAML IdP to be used. The OP SHOULD offer as choices only those IdPs that are known to satisfy the desired assurance requirements.

The SAML LOA profile defines a metadata mechanism by which a SAML IdP can advertise the levels of assurance it is capable of supporting. The OP MAY use the SAML IdP's metadata to retrieve the IdP's assurance certifications.

Once the user has selected an IdP, the OP SHOULD attempt to remember this preference for future use.

In composing a SAML AuthnRequest message to the chosen IdP, the OP should take the PAPE policy URI from the OpenID request and map into an appropriate SAML <RequestedAuthnContext><AuthnContextClassRef> value.

If the original OpenID request specified one of the PAPE defined authentication policies (e.g. phishing-resisistant) in the 'preferred_authn_policies' param, the OP MAY map this policy into an appropriate SAML-defined Authentication Context class URI (e.g. OTP) as the value of the <RequestedAuthnContext> on the SAML AuthnRequest.

If the original OpenID request specified a LOA policy URI in the 'preferred_authn_policies' param, the OP SHOULD map the LOA into an appropriate LOA Authentication context class as per the SAML LOA profile.

Either way, the OP MUST ensure that the specific authentication class or the general LOA requested of the SAML IdP provides equal or greater assurance than specified on the original OpenID request.

4.1.2 Response

Upon receiving the SAML <Response> message from the IdP, the OP SHOULD proxy the SAML message back to the original requesting RP using OpenID. The message MUST be constructed as an OpenID response to the original OpenID request.

If the SAML Response contains a <ProxyRestriction> element with a Count of zero, the IdP MUST NOT proxy the Response message to the OpenID RP. Instead, the OP SHOULD send a negative assertion with openid.mode = "cancel".

If proxying, the OP SHOULD attempt to map any SAML Authentication Context class identifiers from the SAML message into correponding PAPE identifiers on the OpenID response message to the RP.

If the SAML response message specified one of the SAML-defined Authentication Context class URI (e.g. OTP), the OP MAY map this policy into a corresponding PAPE defined authentication policies (e.g. phishing-resisistant). Alternatively, if the SAML response message specified a LOA Authentication Context class (as per the SAML LOA profile) the OP SHOULD map into the appropriate PAPE LOA policy URI in its response to the RP.

Either way, the OP SHOULD ensure that the specific PAPE authentication policy identifier or LOA policy URI on the OpenID reponse to the RP indicates equal or less assurance than provided on the SAML response from the IdP.

If, in the future, the OP is asked to authenticate the user for a different RP, and this request requires equal or less assurance as the original request (as determined by the proxying OP), the OP MAY skip the creation of a new <AuthnRequest> to the SAML IdP and immediately issue another assertion if the original SAML assertion it received from the IdP is still valid.

4.2 User visits SAML SP

4.2.1 Request

If the SAML authentication request contains a <RequestedAuthnContext> that the IdP is unable to satisfy, the IdP MAY proxy the request through OpenID to an OP that can.

If the SAML authentication request contains a ProxyCount value of zero on the <Scoping> element, the IDP MUST NOT proxy the request.

If the SAML authentication request has ForceAuthn = "false" and isPassive = "true", the IdP MUST specify openid.mode = "checkid_immediate" on any proxied OpenID Authentication request.

If the SAML authentication request contains an <IDPList> in the <Scoping> element, the IDP MUST respect the policy and only proxy to any OPs within the list.

If proxying, the IdP SHOULD give the User the ability to choose the OP to be used. The IdP SHOULD offer as choices those OPs that are known to satisfy the desired assurance requirements. The IdP SHOULD use a method for discovering the OP's assurance capabilities that gives it confidence in the OP's abilitiy to meet the desired assurance requriements.

In composing an OpenID authentication request message to the chosen OP, the OP should take the AuthnContext class URI from the SAML request and map into an appropriate PAPE 'preferred_auth_policies' value.

If the original SAML request specified one of the SAML defined authentication class URIs (e.g. OTP), the IdP SHOULD map this policy into an appropriate PAPE defined authentication policy URI (e.g. phishing-resistant).

Alternatively, if the original SAML request specified a LOA class URI as per the SAML LOA profile, the IdP SHOULD map the policy identifier into an appropriate LOA policy identifier within the 'preferred_auth_policies' param on the OpenID request.

Either way, the IdP MUST ensure that the specific PAPE authentication or assurance policy URI requested of the OP provides equal or greater assurance than specified on the original SAML request.

4.2.2 Response

Upon receiving the OpenID response from the authenticating OP, the IdP SHOULD proxy the OpenID message back to the original requesting SP using SAML.

The IdP SHOULD insert an <AuthenticatingAuthority> in the <AuthnContext> of the SAML Assertion returned to the SP. The value of this element MUST be the OP identifier.

The IdP SHOULD attempt to map any URIs in a PAPE 'auth_policies' parameter from the incoming OpenID message into correponding SAML Authentication Context class identifiers on the outgoing SAML <Response> message to the SP.

If the OpenID response message specified one of the PAPE-defined authentication policy URIs (e.g. phishing-resisistant), the IdP MAY map this policy into a corresponding SAML-defined authentication context class URIs (e.g. OTP).

Alternatively, if the OpenID response message specified a PAPE LOA policy URI (either in the PAPE auth_policies or), the IdP SHOULD map into the SAML Authentication Context LOA class URI in its response to the SP.

Either way, the IdP MUST SHOULD ensure that the specific SAML Authentication Context class URI on the SAML response to the SP indicates equal or less assurance than provided on the OpenID response from the OP.

If, in the future, the IdP is asked to authenticate the same user for a different SP, and this request requires equal or less assurance than the original request (as determined by the proxying IdP), the IdP MAY skip the creation of a new OpenID request to the OP and immediately issue another assertion if the original OpenID session is still valid.

5 SECURITY CONSIDERATIONS

TBD

6 REFERENCES

[ICAMOpenID] Bradley, J., "ICAM OpenID 2.0 profile," November 2009 (http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf)

[PAPE] Recordon, D., "Provider Authentication Policy Extension," March 2008 ((http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html)

[SAMLAC] Kemp, J., "SAML Authentication Context," March 2005 (http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)

[SAMLLOA] Cantor, S., Madsen, P., and RL. Morgan,"SAML LOA profile" March 2010 (http://www.oasis-open.org/committees/download.php/32482/sstc-saml-loa-authncontext-profile-draft-03.pdf)