Deployment Profile Requirements Text

(Obviously still draft at this point)

(Mostly expected for inclusion in saml2int, but may require additional review)

Protocol Support

This document describes a deployment profile of certain *SSO Profiles of SAML V2.0* [ref] for deployers of SAML software. Two SAML SSO profiles are constrained by this deployment profile: the SAML V2.0 Web Browser SSO Profile and the SAML V2.0 Single Logout Profile. [ref]

All deployments MUST support the *SAML V2.0 Web Browser SSO Profile* [ref] as specified in this document. A deployment indicates support for SAML V2.0 Web Browser SSO by including certain browser-facing SSO endpoints in metadata.

((What about the SAML V2.0 Single Logout Profile? Is support for SLO required or recommended? In any case, what endpoints in metadata are required and/or recommended?))

((We included HTTP POST in the implementation profile, possibly could include that as a MAY))

~~((Do we have anything to say about the SAML V2.0 Artifact Resolution Profile? No, we left out all the SOAP stuff out of the implementation profile))~~

SP-Initiated SSO

Service Providers must support the direct generation of authentication request messages conforming to the SAML Authentication Request Protocol [SAML Core, 3.4].

Service Providers that want to bypass user-initiated discovery SHOULD support this profile http://docs.oasis-open.org/security/saml/Post2.0/sstc-request-initiation.html

Requiring the use of unsolicited responses (or so called "IdP-initiated SSO requests) is not a substitute for this requirement.

Addresses: Deployment Issue 4; saml2int section: 8.1

SP Deep Link support

Applications that support deep linking and direct addressability of protected resources MUST maintain support for such links in the presence of Web Browser SSO. That is, it MUST be possible to request an arbitrary protected resource and (authorization permitting) have it supplied as the result of a successful SAML SSO profile exchange. In addition, it is RECOMMENDED that Service Providers support the preservation of POST bodies across a successful SSO profile exchange, subject to size limitations dictated by policy or implementation constraints.

The SAML binding-specific RelayState feature is typically used to maintain state required to satisfy both of these requirements, the exact detail of which is left to implementations.

Support for unsolicited responses (or so-called IdP-initiated SSO) is not a substitute for this requirement.

Addresses: Deployment Issue 5; saml2int section: n/a

Clockskew support

Deployers MUST support a minimum of three (3) and a maximum of five (5) minutes of clock skew – in either direction -- when interpreting **xsd:dateTime** values in assertions and enforcing security policies based thereupon.

The following is a non-exhaustive list of items to which this directive applies: `NotBefore`, `NotOnOrAfter`, *and* `validUntil` *XML attributes found on* `Conditions`, `SubjectConfirmationData`, `LogoutRequest`, `EntityDescriptor`, `EntitiesDescriptor`, `RoleDescriptor`, *and* `AffiliationDescriptor` *elements.*

Addresses: Deployment Issue 9, 46; saml2int section: 8.1, 9.1

Keys and Certificates in Metadata

Public keys used for encryption and signature verification are bound to certificates in metadata [ref].

These certificates SHOULD be long-lived and self-signed. To avoid problems with certain non-conforming SAML implementations, certificates in metadata SHOULD NOT be expired.((Do we need an equivalent statement around certificate signature algorithm?))

IdP metadata MUST include at least one signing certificate.

Addresses: Deployment Issue 12; saml2int section: 5

Key and Certificate "Rollover"

SP deployments MUST support multiple signing certificates in IdP metadata. This makes it possible for the IdP to seamlessly migrate to a new signing key.

If the SP publishes an encryption certificate in metadata, the SP deployment MUST be configurable with multiple decryption keys. This makes it possible for the SP to seamlessly migrate to a new decryption key.

Addresses: Deployment issue 11

Endpoints in Metadata

IdP metadata MUST include a `SingleSignOnService` endpoint that supports the SAML2 `HTTP-Redirect` binding. A `SingleSignOnService` endpoin t that supports the SAML2 `HTTP-POST` binding SHOULD also be included in IdP metadata since some SAML SP deployments favor that particular binding. Support for both bindings is strongly RECOMMENDED.

An SP that supports SAML V2.0 Web Browser SSO MUST include at least one `AssertionConsumerService` endpoint that supports the SAML V2.0 `HT TP-POST` binding. Occasionally an IdP will prefer to respond with an artifact, and therefore an `AssertionConsumerService` endpoint that supports the SAML V2.0 `HTTP-Artifact` binding MAY also be included in SP metadata. Note: An SP that supports artifact resolution MUST have at least one signing certificate in metadata.

((We included HTTP POST in the implementation profile, possibly could include that as a MAY))

mdui Elements in Metadata

Metadata for SAML entities MUST include UI elements for mdui:DisplayName, mdui:Logo, mdui:InformationURL, and mdui:PrivacyStatementURL.

The content of the mdui:Logo element SHOULD be a HTTPS URL and MUST NOT be a HTTP URL.

At least one mdui:Logo element SHOULD have a height attribute of 60 and a width attribute of 80.

An entity MAY include a mdui:Logo element with a height attribute of 16 and a width attribute of 16.

Authentication Context requests

An SP that only accepts specific AuthnContextClassRef value(s) in assertions MUST specify those allowable values in the RequestedAuthnContext element of AuthnRequests it generates, with the match attribute set to "exact".

An SP that does not require specific AuthnContextClassRef value(s) in assertions MUST NOT include any RequestedAuthnContext elements in AuthnRequests it generates.

Addresses: Deployment Issue 17; saml2int section: 8.2, 9.2

Attribute Value Constraints

When consuming attributes with standard definitions, Service Providers SHOULD NOT impose constraints that are not part of the definitions of those attributes.

This may imply supporting extra long attribute values, attributes that contain multiple values, broad character set support, etc.

Addresses: Deployment Issue 16, 44; saml2int section: 6, 7

IdP Error URLs

IdP deployers MUST include an `errorURL` XML attribute in metadata. This URL must point to a page that presents actions for a user to take at their organization in response to an error (that occurred at the SP).

Relying parties are encouraged to direct clients to this URL – either directly or after presenting a page providing context – when an authentication error occurs that the Relying Party cannot resolve locally.

Addresses: Deployment Issue 49; saml2int section: 5

Subject ID (Identifier) Value Uniqueness

(Perhaps a preceding item referring to verifying values from IdPs, E.g., qualified attributes, ePSA, ePE, etc.)

SPs MUST be able to prevent inappropriate Subject ID value collisions across different IdPs.

SPs and IdPs SHOULD use qualified identifiers to support this requirement, with the SPs validating that IdPs assert appropriate qualifiers.

((It is RECOMMENDED that the "Scope" Metadata extension be used to support qualified identifiers. *(Is this the correct reference? http://macedir.org/docs /internet2-mace-dir-saml-attributes-latest.pdf)*))

Where IdPs do not assert qualified identifiers for Subject IDs, SPs SHOULD instead internally associate each Subject ID with the asserting IdP's entityID.

Addresses: Deployment Issue 45, 48; saml2int section: 7, 9.2

Subject ID (Identifier) Opaqueness

SPs MUST be able to accept and function reasonably through accepting opaque identifiers. Where necessary, in addition to accepting the user subject ID identifier SPs SHOULD accept one or more relatively unique, human-readable "directory" attributes for use in cases where users are required to identify one another, such as in user searches, user pick-lists, and other interface elements.

Addresses: N/A (identified during identifiers discussions in workgroup)

XML Encryption

~~((Note: we stopped here for the meeting. Tom raised the concern that InCommon doesn't support encryption keys for IdPs.))~~

IdPs MUST support encryption of assertions and SPs must support decryption of assertions using XML Encryption for the Web SSO profile.

~~Deployments that support SLO MUST support encryption (for SPs) and decryption (for IdPs) of NameIDs using XML Encryption for the SLO Profile.~~

Encryption MUST support the AES-GCM cipher for this encryption (XMLENC: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/)

Addresses: Deployment Issue 10; saml2int section: 5, 9.1

Provisioning and Authorization of SAML-only Users (speculative) - NOT ADDED TO SAML2INT YET

Applications that creates new user profile when new a SubjectID is received ("Just In Time", or "On the Fly" provisioning) SHOULD also rely on a separate attribute's value(s) to trigger provisioning of user access. Conversely, absence of that separate attribute, or specific values thereof, should cause user deprovisioning (or deauthorization) to occur.

Deployments SHOULD rely on standard eduPerson attributes intended for this purpose, specifically eduPerson(Scoped)Affiliation and/or eduPersonEntitlement where appropriate.

IdPs MUST NOT be required to block assertions from being generated at the IdP as a substitute for the SP accepting attributes indicating the user's authorization status. *(This may be the actual requirement)*

Addresses: Deployment Issue 7, 8; saml2int section:n/a

Support for Multiple IdPs

Service Providers MUST allow clients the option to authenticate specific resource URLs against more than one identity provider. *(This language is from the Impl Profile)*

When more than one Identity Provider authenticates the same resource URL, IdP selection SHOULD be supported using the `OASIS SSTC SAML v2.0 Identity Provider Discovery Profile`.

((Any comments we should add about discovery bypass?))

Addresses: Deployment Issue 13, 14, 43; saml2int section:8 (or new)

Forced Re-authentication

Identity providers MUST ensure that a request for forced reauthentication (`ForceAuthn="true"`) results in the Subject being required to authenticate in a way that proves that the Subject is present. ((When this condition is met, the IdP MUST reflect this by updating the `AuthnInstant` in its assertion.))

If the IdP cannot prove subject presence, the IdP MUST NOT generate a successful response.

Service Providers SHOULD test the currency of the `AuthnInstant` value contained in the IdP's assertion to verify that it is in fact based on a recent user authentication event.

Addresses: Deployment Issue 35; saml2int section:n/a

IdP Authentication Request Presentation

Service Providers MUST NOT issue authentication requests inside a frame or via any mechanism that would require the use of third-party cookies by the Identity Provider to establish or recover a session with the user agent.

((Is there something broader we want to say about how it SHOULD be presented?))

Addresses: Deployment issue 6

Metadata and Metadata Refresh

Service Providers and Identity Providers MUST regularly verify their SAML peer configurations by validating them against those peers' current metadata. Metadata used for this configuration validation MUST itself be signed and validated with a key distributed (verified? validated?) separately from the metadata itself.

Addresses: Deployment issues 1, 2; saml2int section: 5

SAML EntityIDs

The EntityID of a SAML entity MUST be scoped to the domain of the organization that the owner of the application, in the case of an SP; or the owner of the organization whose users are represented by the IdP, in the case of an IdP.

Specifically, hosted applications must have entityIDs scoped to the client organization's domain, not the host's domain.

((Probably needs more clarity.))