WebSSO Scalable Federation Implementation Profile

```
:numbered:
```

Table of Contents

```
:toc:
```

1. Message Flows and Bindings

Table 1. Support for the combination of message flows, bindings and message authentication

RequID	IDP	SP	Source	Message Flow	Binding	Message AuthN
IMFB-001	MUST	MUST	eGov W241	Web SSO AuthnRequest (see [SAML2Prof] sect. 4.1)	HTTP redirect	Signature
IMFB-002	MUST	MUST	eGov W274, 290	Web SSO Response (see [SAML2Prof] sect. 4.1)	HTTP POST	Assertion signature
IMFB-003	MAY	MAY	eGov W274, 290	Web SSO Response (see [SAML2Prof] sect. 4.1)	HTTP POST	Response signature
IMFB-004	MUST	MUST	eGov W274, 290	Web SSO Response (see [SAML2Prof] sect. 4.1)	HTTP artifact	Signature
IMFB-005	MUST	MUST	eGov W274, 290	Web SSO unsolicited Response (see [SAML2Prof] sect. 4.1.5)	n/a	n/a
IMFB-006	MUST	MUST	eGov A323, 330, 331	Artifact Resolution Request and Response (see [SAML2Prof] sect. 5)	SOAP	Message signature
IMFB-007	MUST	MUST	eGov A323, 330, 331	Artifact Resolution Request and Response (see [SAML2Prof] sect. 5)	SOAP	TLS
IMFB-008	MUST	MAY	eGov S377, 384	SP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	HTTP redirect	Message signature

RequID	IDP	SP	Source	Message Flow	Binding	Message AuthN
IMFB-009	MUST	MUST	eGov SLO 317, 384	SP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	SOAP	Message signature
IMFB-010	MUST	MUST	eGov SLO 315, 384	IdP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	SOAP	Message signature
IMFB-011	MUST	MAY	eGov SLO 317, 384	SP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	HTTP redirect	TLS
IMFB-012	MUST	MUST	eGov SLO 317, 384	SP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	SOAP	TLS
IMFB-013	MUST	MUST	eGov SLO 315, 384	IdP-initiated LogoutRequest (see [SAML2Prof] sect. 4.4)	SOAP	TLS
IMFB-014	MUST	MAY	eGov SLO 405, 410, 414	IDP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	HTTP redirect	Message signature
IMFB-015	MUST	MUST	eGov SLO 405, 410, 414	IDP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	SOAP	Message signature
IMFB-016	MUST	MUST	eGov SLO 405, 410, 414	SP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	SOAP	Message signature
IMFB-017	MUST	MAY	eGov SLO 405, 410, 414	IDP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	HTTP redirect	TLS
IMFB-018	MUST	MUST	eGov SLO 405, 410, 414	IDP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	SOAP	TLS
IMFB-019	MUST	MUST	eGov SLO 405, 410, 414	SP-initiated LogoutResponse (see [SAML2Prof] sect. 4.4)	SOAP	TLS
IMFB-020				IDP Discovery (see [IdPDisco] sect. 2.4.1)	(cookie)	Message signature
IMFB-021				Request Initiation Protocol (see [SAML-ReqInit])	HTTP GET	

RequID	IDP	SP	Source	Message Flow	Binding	Message AuthN
IMFB-022				Assertion Query AttributeQuery (see [SAML2Prof] sect. 6)	SOAP	
IMFB-023				Enhanced Client/Proxy SSO (see [SAML2Prof] sect. 4.2)	PAOS	
IMFB-024				Name Identifier Management (IdP-initiated) (see [SAML2Prof] sect. 4.5)	HTTP redirect	
IMFB-025				Name Identifier Management (IdP-initiated) (see [SAML2Prof] sect. 4.5)	SOAP	
IMFB-026				Name Identifier Management (SP-initiated) (see [SAML2Prof] sect. 4.5)	HTTP redirect	
IMFB-027				Name Identifier Management (SP-initiated) (see [SAML2Prof] sect. 4.5)	SOAP	
IMFB-028				Holder-of-Key WebSSO (see [SAML2HoK])		

2. Message Encryption

In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the generation and consumption of <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500]. The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an alternative.

Table 2. Supported SAML message encryption modes

RequID	IDP	SP	Source	Requirement
ATR-001	MUST	MUST	eGov/227	Support attribute name format urn:oasis:names:tc:SAML:2.0:attrname-format:uri (see [SAML-X500] sect. 2.3)
ATR-002	MUST	MUST	eGov/231	Support xs:string as attribute values; other types are optional (see [SAML2Core] sect. 2.7.3.1.1)
ATR-003	?	?	new	Supply/consume explicit xs:type for <AttributeValue> (see [SAML2Core] sect. 2.7.3.1.1)

3. Attribute Name Formats

In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the generation and consumption of <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500]. The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an alternative.

Table 3. Supported SAML attribute elements

RequID	IDP	SP	Source	Requirement
ATR-001	MUST	MUST	eGov/227	Support attribute name format urn:oasis:names:tc:SAML:2.0:attrname-format:uri (see [SAML-X500] sect. 2.3)
ATR-002	MUST	MUST	eGov/231	Support xs:string as attribute values; other types are optional (see [SAML2Core] sect. 2.7.3.1.1)
ATR-003	new?	new?	-	Supply/consume explicit xs:type for <AttributeValue> (see [SAML2Core] sect. 2.7.3.1.1)

4. Name Identifier Formats

In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

Table 4. Supported SAML Name Identifier formats

RequID	IDP	SP	Source	Format Identifier
NID-001	MUST	MUST	eGov/223	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent (see [SAML2Core] sect. 8.3)
NID-002	MUST	MUST	eGov/224	urn:oasis:names:tc:SAML:2.0:nameid-format:transient (see [SAML2Core] sect. 8.3)

5. SAML Metadata

5.1. Metadata Profiles and Capabilites

Table 5. Supported SAML metadata profiles and capabilites

ReqID	IDP	SP	DS	Source	Requirement
MD-100	X	X		InC Draft	MUST support SAML V2.0 Metadata [SAML2MD] as updated by Errata [SAML2Errata]
MD-101	X	X		InC Draft	MUST support SAML V2.0 Metadata Schema [SAML2MD-xsd]
MD-102	X	X	X	eGov/163	MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [SAML2MDIOP].
MD-103	X	X	X	InC Draft	Per [SAML2MDIOP], all run-time configuration of SAML profiles (technical trust and general operational configuration) MUST be manageable via SAML metadata alone. Further, it MUST be possible to configure an IdP or SP to allow basic interop with any peer for which metadata is supplied, without intervention by the deployer.
MD-104	X	X	X	eGov/167	MUST support the <ds:X509Certificate> element as key representation int the <md:KeyDescriptor> element
MD-105	X	X		InC Draft	Per [SAML2MDIOP], support for any number of long-lived, self-signed end entity certificates is REQUIRED, as is support for expired certificates, and certificates signed with any digest algorithm.
MD-106	X	X	X	eGov/168	Support for other key representations than <ds:X509Certificate>, and for other mechanisms for credential distribution, is OPTIONAL
MD-107	X	X	X	eGov/170	MUST support some form of path validation of signing, TLS, and encryption credentials used to secure SAML exchanges against one or more trusted certificate authorities.
MD-108	X	X	X	eGov/172	Support for PKIX [RFC5280] is RECOMMENDED. Implementations SHOULD document the behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280]

RequID	IDP	SP	DS	Source	Requirement
MD-109	X	X	X	eGov/176	MUST support the use of OCSP [RFC2560] and Certificate Revocation Lists (CRLs) obtained via the 'CRL Distribution Point' X.509 extension [RFC5280] for revocation checking of those credentials.
MD-110	X	X	X	eGov/179	MAY support additional constraints on the contents of certificates used by particular entities, such as 'subjectAltName' or 'DN', key usage constraints, or policy extensions, but SHOULD document such features and make them optional to enable where possible.
MD-111	X	X	X	eGov/186	SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.
MD-112	X	X		InC Draft	Key Rollover: MUST be able to consume and utilize two or more signing keys bound to a single role descriptor in metadata. To verify a signature, an implementation MUST try each signing key (in unspecified order) until the signature is verified or there are no more signing keys (in which case signature verification fails).
MD-113	X	X		InC Draft	Key Rollover: MUST be able to consume and utilize two or more encryption keys bound to a single role descriptor in metadata. To encrypt a message, any encryption key in metadata MAY be used. If there are multiple encryption keys of a given type in metadata, the implementation may choose any one of them at its discretion and need not explicitly define which one will be used.
MD-114	X	X		InC Draft	Key Rollover: If an implementation supports inbound encryption, it MUST itself be configurable with up to two decryption keys (this is not a metadata requirement but applies to the configuration of keys used by the implementation).
MD-115	X	X		InC Draft	An <md:KeyDescriptor> element in metadata that contains no use XML attribute MUST be valid as either a signing or encryption key.
MD-116	X			new	MUST support the grouping of SPs by Entity Categories [SAMLEntityCat] and base policy decisions on Entity Categories

RequID	IDP	SP	DS	Source	Requirement
MD-117	X			new	MUST support the release of a minimal attribute set based on an Entity Category value [SAMLEntityCat] in absence of <md:RequestedAttribute> elements.
MD-118	X			new	MUST support the release of an attribute set based on an Entity Category value [SAMLEntityCat] that is the intersection of the SP’s <md:RequestedAttribute> elements and a set of attributes defined fo the Entity Category

5.2. SAML Metadata Exchange

Table 6. Requirements for SAML metadata exchange

RequID	IDP	SP	DS	Source	Requirement
MD-200	X	X	X	eGov/190	Support for the generation or exportation of metadata is OPTIONAL.
MD-201	X	X	X	eGov/191	MUST support the publication of metadata using the Well-Known-Location method defined in section 4.1 of [SAML2Meta] (under the assumption that entityID values used are suitable for such support).
MD-202	X	X	X	eGov/196	MUST support the importation of metadata from a local file.
MD-203	X	X	X	eGov/197	MUST support the importation of metadata from a remote resource at fixed location accessible via HTTP 1.1 or HTTP 1.1 over TLS/SSL. Implementations MUST support use of the 'ETag' and 'Last-Modified' headers for cache management.
MD-204	X	X	X	eGov/200	SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a single entity’s metadata is present in more than one source.
MD-205	X	X	X	eGov/203	Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MUST be supported.
MD-206	X	X	X	eGov/205	SHOULD allow for the automated updating/reimportation of metadata without service degradation or interruption.
MD-207	X	X	X	eGov/208	Verification of metadata, if supported, MUST include XML signature verification at least at the root element level

RequID	IDP	SP	DS	Source	Requirement
MD-208	X	X	X	eGov/211	Verification of metadata SHOULD support direct comparison against known keys.
MD-209	X	X	X	eGov/212	Verification of metadata SHOULD support some form of path-based certificate validation against one or more trusted certificate authorities, along with certificate revocation lists and/or OCSP [RFC2560]. Support for PKIX [RFC5280] is RECOMMENDED. Implementations SHOULD document the behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].
MD-210	X	X	X	InC Draft	MUST support metadata verification based on the presence of the validUntil XML attribute, and MUST have the ability to enforce limitations on the duration of validity (e.g., it must be possible to block consumption of metadata without such an attribute or one that is too far into the future)
MD-211	X	X	X	eGov/208	Verification of metadata, if supported, MUST include XML signature verification at least at the root element level
MD-212	X	X	X	eGov/211	Verification of metadata, if supported, SHOULD support the direct comparison against known keys as mechanism for signature key trust establishment.
MD-213	X	X	X	eGov/212	Verification of metadata, if supported, SHOULD support Some form of path-based certificate validation against one or more trusted certificate authorities as mechanism for signature key trust establishment. Certificate revocation lists and/or OCSP [RFC2560] and support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].

6. IDP Discovery

Table 7. Supported IDP discovery protocols

RequID	IDP	SP	Source	Requirement
DIS-001	MUST	MUST	eGov/227	MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

7. SAML WebSSO Message Formats

Support for the SAML V2.0 Web Browser SSO Profile [SAML2Prof] is required with following capabilites.

Table 8. SAML Authentication Request

RequID	IDP	SP	Source	Requirement
SSO-001		MUST	eGov/249	MUST support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes (when appropriate): ---- * AssertionConsumerServiceURL * ProtocolBinding * ForceAuthn * IsPassive * AttributeConsumingServiceIndex * <saml2p:RequestedAuthnContext> * <saml2p:NameIDPolicy> ----
SSO-002	MUST		eGov/249	MUST support all <saml2p:AuthnRequest> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options.
SSO-003	MUST		eGov/249	MUST fully support the options enumerated below, and be configurable to utilize those options in a useful manner as defined by [SAML2Core].: ---- * AssertionConsumerServiceURL * ProtocolBinding * ForceAuthn * IsPassive * AttributeConsumingServiceIndex * <saml2p:RequestedAuthnContext> * <saml2p:NameIDPolicy> ----
SSO-004	MUST		eGov/264	MUST support any allowable content of the <saml2p:RequestedAuthnContext> element but MAY limit

RequID	IDP	SP	Source	Requirement
				their support of the element to the value "exact" for the Comparison attribute.
SSO-004	MUST		eGov/268	MUST support verification of requested AssertionConsumerServiceURL locations via comparison to <md:AssertionConsumerService> elements supplied via metadata using case-sensitive string comparison. It is OPTIONAL to support other means of comparison (e.g., canonicalization or other manipulation of URL values) or alternatve verification mechanisms. ----