The initial draft of the saml2int profile reformatted for Kantara is [here]. If you currently link to the old saml2int.org copy of this profile, you should revise your links because Kantara is the owner of the authoritative copy.

At present, active discussion to substantially revise saml2int is taking place within the InCommon Deployment Profile WG, which will make a set of change proposals to Kantara to revise this profile. This is expected by the end of 2017.

A first major piece of this work is a submission to OASIS to define a new identifier strategy for SAML, which we will propose as a required element of a new saml2int.

A set of older, largely historical issues identified are below.

Suggested Changes (mostly from older discussions amongst Ian/Scott/Andreas):

- Add to section 3 after line 85:

```xml
Any <md:RequestedAttribute> elements representing attributes to be exchanged using SAML 2.0 MUST have a Name Format of "urn:oasis:names:tc:SAML:2.0:attrname-format:uri". Additional <md:RequestedAttribute> elements MAY be present if they are to be used in other protocols and include appropriate NameFormat values. The NameFormat attribute MUST NOT be omitted on any such elements.
```

- Modify section 6.1, lines 147-148:

```xml
Identity Providers MAY omit the verification of signatures in conjunction with this binding, and SHOULD NOT impose a requirement for signed requests. Identity Providers MAY support enhanced functionality in the presence of signed requests.
```

- In section 2, the first three syntax examples use placeholder names while the last one uses a real element name. Should be made consistent. If we use the placeholder names, prefer ProtocolElement rather than ProtocolElement.

- Line 70, s/its entity/their entities
- Line 73, s/its metadata/their metadata
- Lines 91-93: replace with:

```xml
Each <md:SingleSignOnService> and <md:AssertionConsumerService> endpoint supported by an Identity Provider or Service Provider, respectively, MUST be protected by TLS/SSL.
```

- In section 6.1, line 150, change SHOULD to MUST.

- In section 7.1, replace lines 182-190 with:

```xml
The endpoint(s) at which a Service Provider receives a <saml2p:Response> message MUST be protected by TLS/SSL. If supported by an SP, Identity Providers MAY utilize XML Encryption and return a <saml2:EncryptedAssertion> element in the <saml2p:Response> message. The use of the <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is NOT RECOMMENDED; when possible, encrypt the entire assertion (if at all).

The <saml2:Response> element issued by the Identity Provider MUST be signed directly using a <ds:Signature> element within the <saml2:Response>. The <saml2:Assertion> element MAY also be signed directly if required for reasons other than the use of this profile.
```

- In section 7.1, replace lines 191-192 with "Service Providers MAY reject unsolicited <saml2p:Response> messages."

- In section 7.2, lines 197-198, reword as "MAY contain one <saml2:AttributeStatement> element."

- Extrapolate all required metadata content based on other profile requirements and explicitly enumerate those required elements. For example, since POST is a required binding for SPs, at least one ACS for that binding has to be present.