Staging service

Problem statement

- Service Providers outside EU/EEA (and Identity Providers in EU/EEA) must commit to the international Data protection Code of Conduct (iCoCo).
- the iCoCo is a strong commitment for a non-EU/EEA SP because they volunteer to be bound by European data protection laws
  - unlike the Home Organisations and SPs in EU/EEA who are bound by the European laws anyway
- therefore, the evidence of the commitment must be strong enough
- Example dispute scenario:

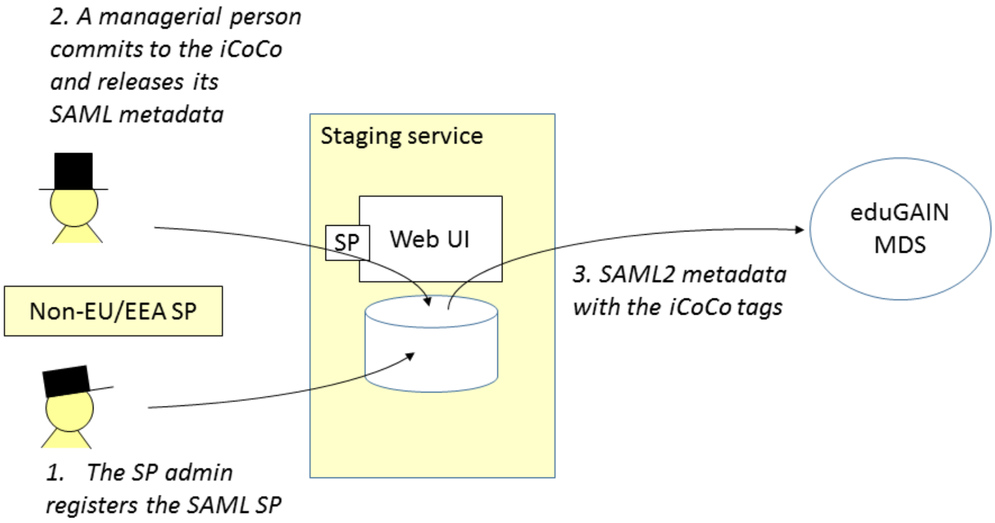
1. the SP admin asks his/her boss if it is OK to commit to the iCoCo. The boss says carelessly “yes”
2. the next day the boss has studied the issue more, changed his/her mind and says that s/he hasn’t ever heard of the iCoCo and if s/he had s/he wouldn’t have ever allowed the organization to commit to the CoCo

Alternative solutions (from strong to weak evidence)

1. The SP-organisation needs to present a paper with wet or qualified e-signature from a management level person saying “we are committed to the Code of Conduct and I’m a truly representative person of the organization”
2. The manager level person needs to log in to something using his/her personal account and click a button saying “we are committed to the Code of Conduct and I’m a truly representative person of the organization”. Pressing the button is logged.
3. The manager level person needs to send email to someone in eduGAIN to say “we are committed to the Code of Conduct and...
4. We have what we have for the GÉANT CoCo at the moment. Only element in SAML2 metadata and a link in the privacy policy document.

Proposed solution (alternative 2)

- There is an iCoCo Staging service that is registered as an SP to relevant (non-EU/EEA) federations
  - the Staging service must be able to trust the users authenticated from non-EU/EEA IdPs
  - the Staging service must be able to receive sufficient PII attributes from the IdP
- The iCoCo staging service is part of or is closely coupled to the SAML2 metadata management service of an eduGAIN participant federation


2. A managerial person commits to the iCoCo and releases its SAML metadata
Staging service
SP
Web UI
eduGAIN MDS
3. SAML2 metadata with the iCoCo tags
Non-EU/EEA SP
1. The SP admin registers the SAML SP

- The non-EU/EEA SP goes through the following workflow to commit to the international CoCo

1. The SP administrator submits the SP's SAML2 metadata to the Staging service
2. A truly representative person from the Service Provider organization logs in to the Staging service selects the SP and clicks a button “we are committed to the Code of Conduct and I’m a truly representative person of the organization”. Clicking the button is logged for audit trail.
3. The Staging service releases the SP's SAML2 metadata to eduGAIN Metadata service (MDS), with the Entity Category tags indicating commitment to the iCoCo

Proposed technical implementation

- policy-wise, the requirements of the Staging Service are spelled out the related Entity Category Specification as requirements for the registrar
- technically, a Staging service can be provided
  - by one or several eduGAIN participant federations in Europe or beyond
  - by a federation which is dedicated for registering non-European SPs to eduGAIN