

PEER Project Plan and Proposal

Contents

- 1 [Contents](#)
 - 2 [Background](#)
 - 3 [Goals](#)
 - 4 [Architecture and Scope](#)
 - 5 [Governance](#)
 - 6 [Plan](#)
 - 7 [Budget](#)
- [PEER Project Phase 1](#)
 - [PEER Project Phase 2](#)
 - [PEER Project Phase 3](#)
 - [PEER Software Backlog](#)

Background

This is a plan for a project to develop and establish a metadata registry based on the [PEER User Stories](#) and [PEER Service Description](#). The PEER service and software draws from years of accumulated knowledge and is based on user-stories developed by representatives from WAYF.dk, MACE, InCommon, The UK Access Management Federation and SWAMID.

PEER aims to be a lightweight solution for the registration of SAML Metadata. PEER approaches SAML metadata differently from the well known and understood access management federations. Most federations in operation now:

- Offer both technical trust and behavioural trust (through policy management);
- Provide both metadata registration and metadata publication services.

PEER will provide only technical trust and metadata registration, and leaves the other considerations for consumers of the metadata to manage.

In order to ensure optimum use of federated access management, it is important that both ends of the security spectrum are examined. Whilst international efforts such as eduGain are examining this space from a policy driven perspective, PEER seeks to examine an approach where the registrar of the metadata does not involve itself in establishing policies for consumption.

The PEER service will provide the opportunity to examine the necessity of behavioural trust, challenge the current model of registration and publication as a central service for federations and review the points at which trust is established between end users and relying parties. This in turn will provide opportunities to improve the services offered by federations and provide economies of scale through a shared registration service for federations and support for more effective management of metadata.

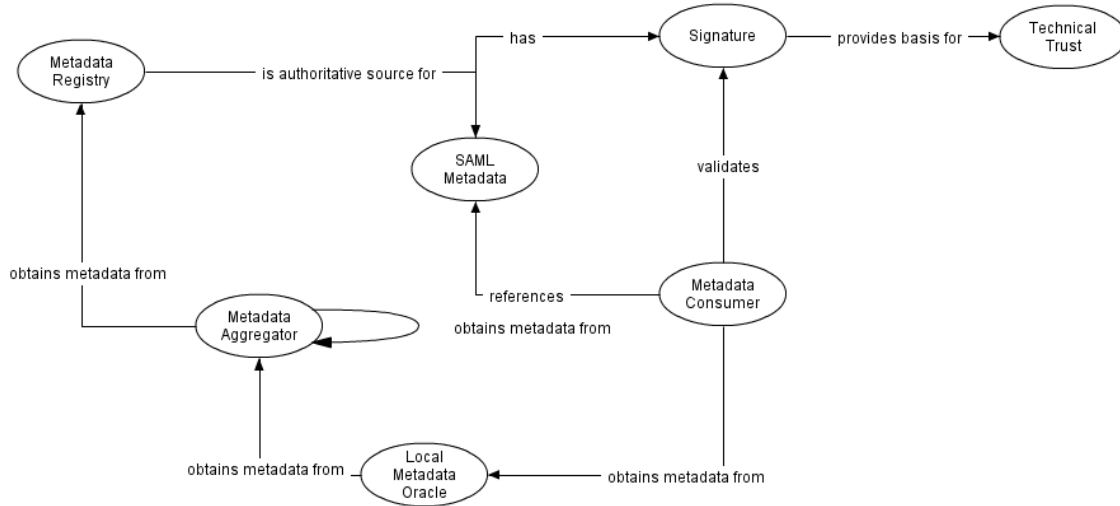
Goals

The goals of the PEER project are:

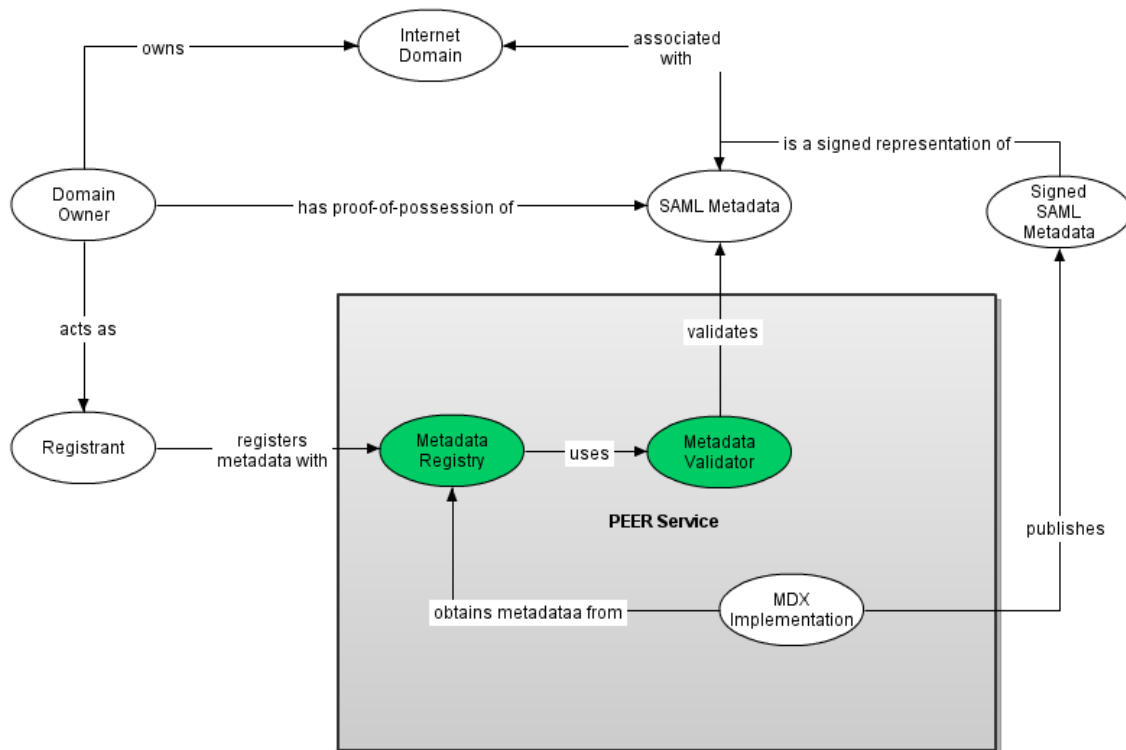
- To develop a software package based on the PEER user-stories.
- To deploy the PEER software in combination with other software and tools (cf below) as a service fulfilling the PEER service description.
- To develop proposals for the long-term sustainability of PEER.

Architecture and Scope

The following diagram illustrates a reference model of metadata distribution. In this model, the PEER service is an instance of a metadata registry. Where it is unambiguous the word metadata refers to SAML metadata. Note that not all instances of SAML metadata entities describe SAML protocol endpoints - the PEER service is meant to be agnostic wrt the uses of the SAML metadata within the registry.



The following diagram illustrates the scope of the software developed for the PEER project and the role of a registrar in the federation model. The diagram is in the form of an ontology diagram. Read each ellipse-arrow-ellipse as a sentence, eg "A domain owner has a proof-of-possession of SAML metadata" or "The MDX implementation obtains metadata from the metadata registry" and "The MDX implementation publishes signed metadata.



The PEER service (the grey box) will perform the following functions (the PEER service description provides a full list) :

1. Validate that the registrant owns the metadata it is trying to register
2. Validate that the registered metadata is syntactically (and to some extent semantically) correct
3. Store the metadata in a metadata repository where it can be retrieved by an MDX implementation for publication.

In particular the following are expected to be out of scope for the PEER software (but not for the PEER service):

1. Signing metadata and publishing signed metadata. This will be the responsibility of an MDX implementation TBD.
2. Implement all aspects of a fully functional metadata store. Metadata is expected to be stored in either a general purpose VCS (version control system) or in some form of XML store abstraction layer which supports indexed retrieval of individual entities. Depending on the tools available the PEER software may need to provide indexing and searchability of metadata.

The components marked in green represent those software components which are expected to be part of the PEER software development project.

Governance

In accordance with agile methods best practices a product owner will be identified to act as a liaison between the future users of the PEER software and service and the developers. The product owner will chair the project reference group and will be responsible for evolving and prioritizing the user-stories between each development sprint.

Additionally a project steering group will be responsible for oversight and budget control.

The project team is made up of the following people:

- Project Manager: Nicole Harris.
- Product Owner: Leif Johansson.
- Shibboleth Team: Chad La Joie and Ian Young.
- Yaco Team: ??.

The steering group for the project is:

- Ken Klingenstein, Internet2.
- Licia Florio, TERENA (TERENA representative).
- Lucy Lynch, ISOC (funder representative).
- Victoriano Giralt, UMA.
- David Simonsen, WAYF.

Plan

The project consists of 3 phases:

1. [Planning](#) (October 2010 - February 2011);
2. [Development](#) (April 2011 - September 2011);
3. [Service deployment](#) (September 2011 - December 2011).

Four work-areas will run across these phases to ensure consistency and co-ordination"

1. Project Management;
2. PEER User Interface;
3. PEER Storage Engine and Metadata Validator;
4. Support and Delivery.

The planning phase of the project began in October 2010 with the identification and articulation of user stories. The development-phase of project will use SCRUM and will consist of a number of coding sprints. As the code for the PEER software starts to form the service deployment phase will start. During this phase new releases from the code sprints will be deployed in a pre-production environment.

The PEER service is intended to be operated in more than once instance and the software will be made available under a BSD or comparable OpenSource License as soon as possible after the development phase of the project is underway.

At least two instances will be run during the Development and Service Deployment phase:

- SWAMID will operate an instance of PEER for internal use;
- NORDUnet will operate a public instance of PEER;
- The UK will run a public instance of PEER.

Budget

| Budget Amount | Funded Party | Work Areas | Deliverables |
|---------------|--------------|------------|--------------|
|---------------|--------------|------------|--------------|

| | | | |
|------------------------------|---|---|---|
| \$37,300 | Yaco Sistemas | Development and Delivery of PEER User Interface. Funding will be used to provide approximately 330 hours of development time from Yaco Sistemas plus contributions to bi-weekly conference calls and full involvement in sprint testing. | <ul style="list-style-type: none"> • PEER UI software, fully packaged and delivered under BSD license. • Documentation to support the PEER software, to be maintained on the I2 wiki. |
| \$5,000 | WAYF.dk | Development and Delivery of PEER use cases. Funding will be used to support the development of the PEER use cases plus contributions to bi-weekly conference calls. | <ul style="list-style-type: none"> • Maintenance and development of the PEER User Stories to inform development requirements. • PEER documentation for end-users, focused on use-case scenarios. |
| \$8,400 | Shibboleth Consortium | Development and Delivery of PEER storage engine and metadata validator. Funding will be used to provide approximately 80 hours of development time from the Shibboleth Consortium plus contributions to bi-weekly conference calls and participation in sprint testing. | <ul style="list-style-type: none"> • Storage Engine and metadata validator delivered under Shibboleth license. • Documentation to support the metadata validator. |
| \$7,000 (NH) \$1,400 (IY) | Nicole Harris, Leif Johansson and Ian Young | Product and project management including full development of project plans, oversight of the coding sprints, development of appropriate user documentation and recommendations for future service delivery. | <ul style="list-style-type: none"> • PEER project plan. • Coordination of bi-weekly teleconferences. • Coordination of coding sprints. • Development of appropriate terms of use and trust model for PEER. • PEER documentation for federations. • PEER documentation for entities. • Recommendations for future service delivery. |