Inter-Federation & GÉANT 3 eduGAIN

Reaching beyond national borders

SWITCH

Serving Swiss Universities

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Bern, 16. September 2009

Overview

1. What's the Problem?
2. GÉANT 3 eduGAIN
3. Scalable Metadata Exchange
4. Metadata Tagging
5. Summary

What's the Problem?

- The fact
  - More and more national Identity Federations based on SAML
- The problem
  - How to establish 'Schengen' for Identity Federations?
    - Borders still exist, but they are no longer barriers
- Two technical topics which should finally ease Inter-Federation
  - Scalable Metadata Exchange
  - Metadata Tagging

GÉANT 3 eduGAIN

- In GÉANT 2 eduGAIN was a pilot for inter-federation
  - Starting point was: Federations use various protocols
  - In the mean time, SAML 2 as standard accepted
  - No bridging elements needed anymore to translate protocols
  - SWITCH participated with hosts from the AAI Test Federation

- In GÉANT 3 eduGAIN will become a service
  - Planned to become operational in summer 2010
  - First only a pan-european WebSSO service
  - Mainly policies and technical details need to be solved

- *GÉANT 2: 2006 - 2009*
- *GÉANT 3: 2009 - 2012*

Credits

- All the following is primarily based on the work and feedback of
  - Chad La Joie, SWITCH & Internet2
  - Ian A. Young, SDSS
  - Leif Johansson, Stockholm University
  - Scott Cantor, The Ohio State University & Internet2

  &many more from GÉANT2 JRA5 and elsewhere

- Its all work in progress…

Scalable Metadata Exchange

- Federations grow ⇒ Metadata files grow
- Inter-Federation ⇒ Single Metadata file unmanageable

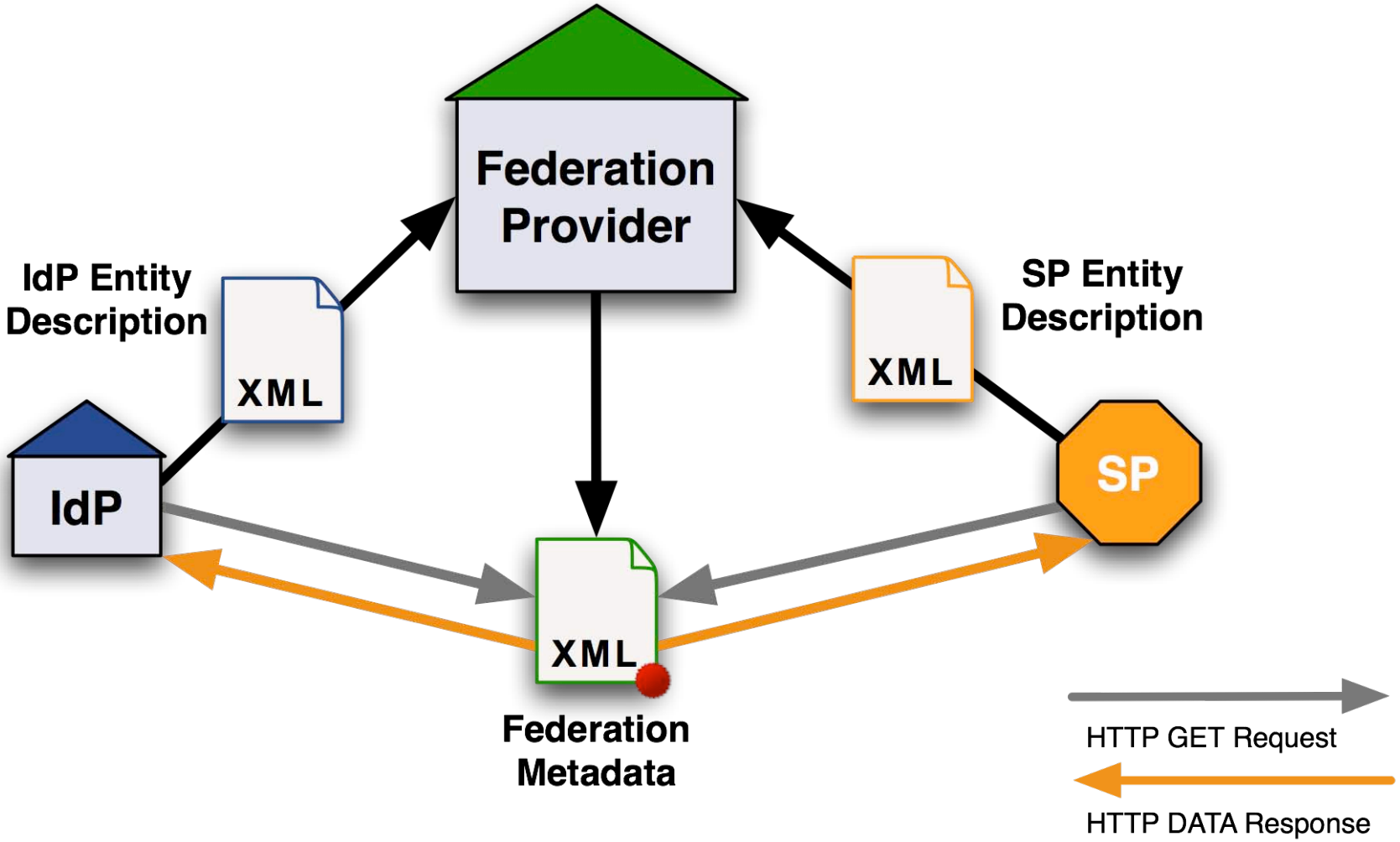
- Direct SAML2 based end-to-end communication should be maintained

- Idea: Each entity needs just the set of metadata of its communication partners

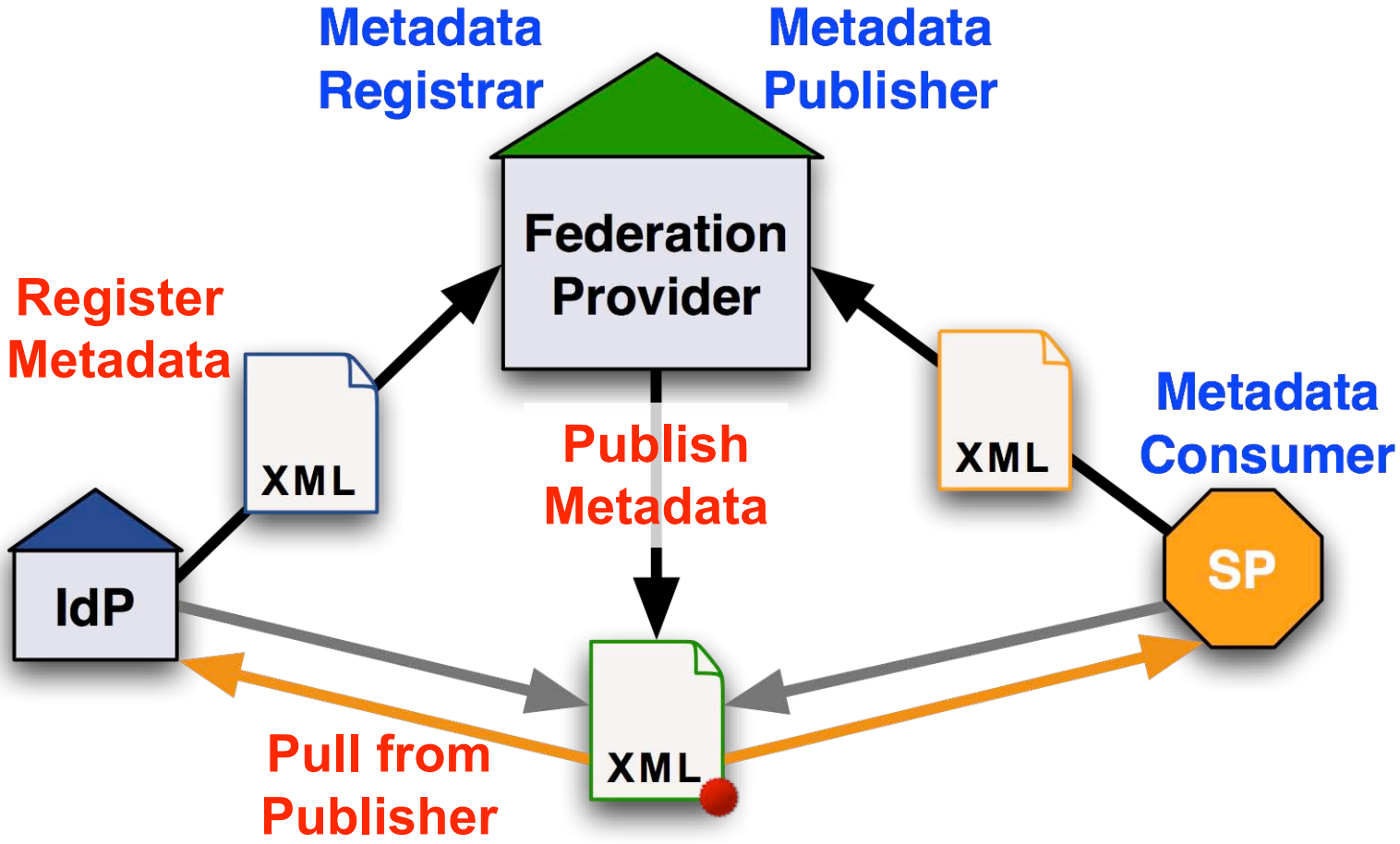
See also: Interfederation and Metadata Exchange: Concepts and Methods

http://www.iay.org.uk/blog/2009/05/concepts_and_me.html

Federation Metadata today



Federation Metadata today (2)



What is the role of Federations?

- A Federation offers a set of services
  - Legal and/or policy framework
    ⇒ Supports trust
  - Technical recommendations or standards to deploy
    ⇒ Eases interoperability
  - Metadata management
  - Provide tools & support

- A Federation provides **some scalability**
  - for `m` IdPs and `n` SPs
    - only `m+n` relationships with the Federation Provider
    - instead of up to `m*n` direct relationships

Federations are Trust Brokers

- Distinguish two kinds of trust

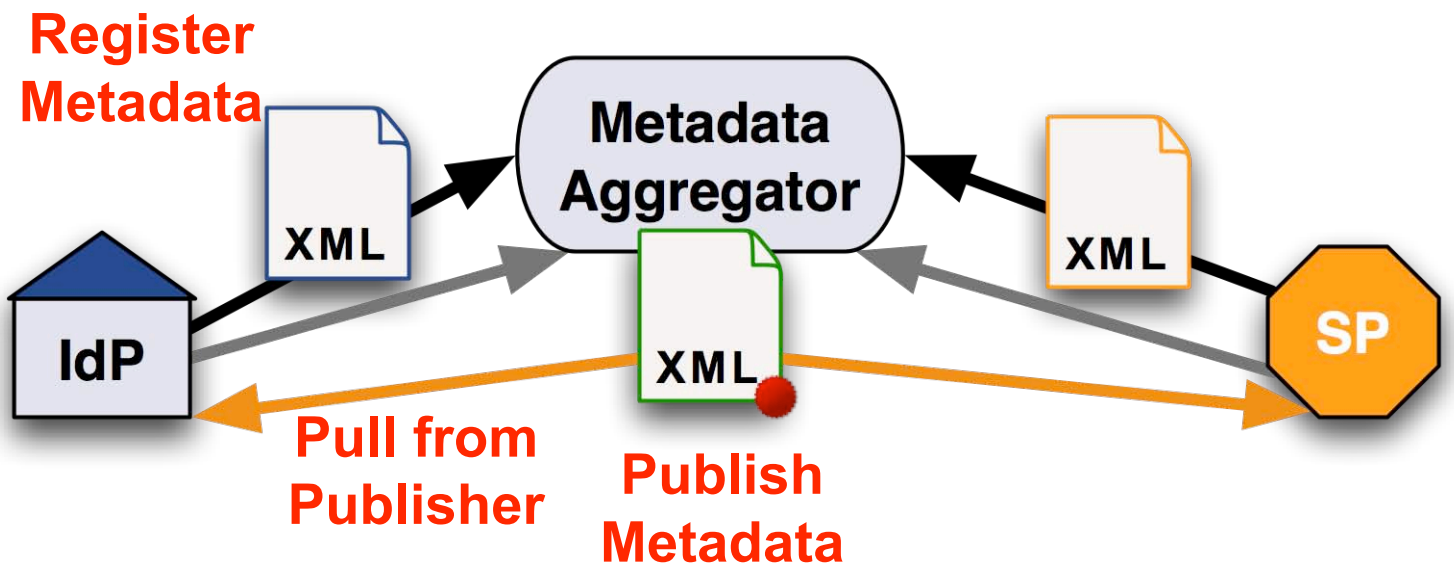
- **Technical Trust**
  - Trustworthy entity metadata
    ⇒ Assures secure communication between the entities

- **Behavioural Trust**
  - Requires proper technical trust as basis
  - Comprises what is settled by contract or policy
    - e.g. quality of Identity Management
    - Correctness of attribute values asserted

Crossing the Federation Borders

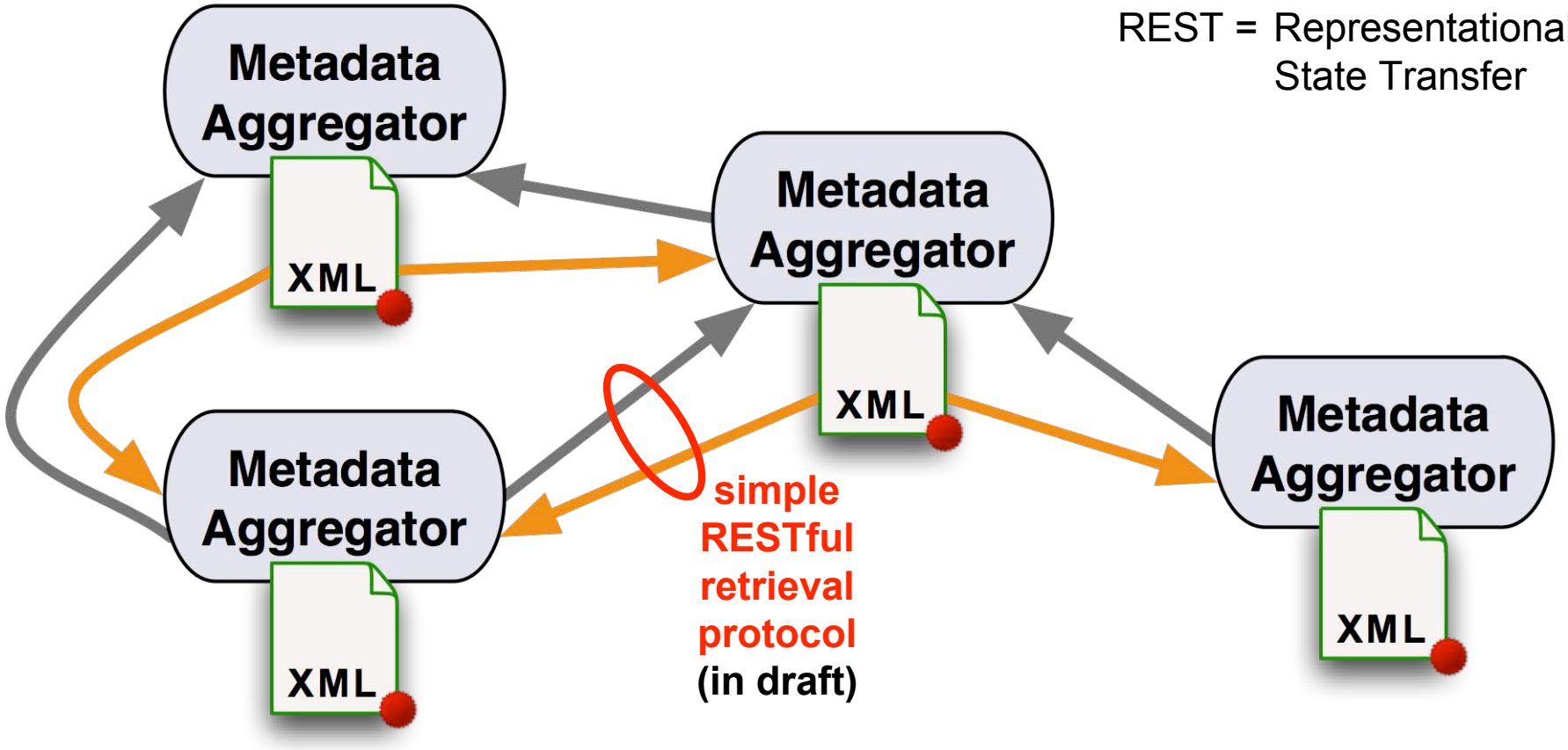
- Technical Trust for Inter-Federation
  - Introduce a ‘Metadata Layer’ for trustworthy access to entity metadata
- Metadata Aggregator
  - aggregates metadata from metadata publishers
    - *Process to be documented in an Aggregation Practice Statement*
  - optionally accepts entity registrations
    - *Process to be documented in a Registration Practice Statement*
  - publishes metadata for consumers
- Entities
  - register their own metadata with a Metadata Aggregator
  - consume their metadata entity collection from a Metadata Aggregator

Metadata Aggregation



A Federation Provider is a Metadata Aggregator

Metadata Layer



- Scalability through a mesh of Metadata Aggregators
- Entities to choose their preferred Metadata Publisher, matching their needs

Components of an Aggregator

- Metadata Registrar
  - Register metadata from client entities
- Metadata Subscription
  - Fetch metadata from other aggregators
- Transform metadata
  - Filter entities on suitable criteria
- Merge metadata
- Publish metadata
  - universally
    - ‘Locally’ registered metadata which want to inter-federate
  - to client entities and selected aggregators
    - Specific entity-collections - filtered sets of entities

Metadata Tagging

- Why to tag entities in metadata?
  - Describe the entity in a way suitable for **filtering**
  - Third party **asserts** that an entity meets some **qualification**
- Tags in use by the UK federation
- Use XML extension mechanism for not breaking metadata interoperability
  - Scott Cantor submitted a proposal for introducing **Entity Attributes** suitable as tags for entities in metadata
    - For all details see the spec at OASIS, currently Committee Specification 01: SAML V2.0 Metadata Extension for Entity Attributes Version 1.0

http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html

`EntityAttributes`: What is it?

- The **`<mdattr:EntityAttributes>`** element is a **wrapper** for one or more **`<saml:Attribute>`** or **`<saml:Assertion>`** elements.
  - Assertions MUST conform to the assertion profile and will contain only attribute statements.
    - Assertion profile:
      The value of the **`<saml:NameID>`** MUST correspond to the **`entityID`** of the enclosing **`<md:EntityDescriptor>`** element. (…)
  - Relying parties MUST process assertions in accordance with the standard processing rules in [SAML2Core].

- If the **`EntityAttributes`** element is used within the **`<md:Extensions>`** element of an **`<md:EntityDescriptor>`** element, then it binds the enclosed SAML attributes (or the attributes within the enclosed assertions) to the enclosing entity. (…)

Tagging Entities with Entity Attributes

- To become useful, appropriate attributes for describing entities have to be defined
  - A job for the federations and the bodies coordinating inter-federation

- Assertion for an entity by a third party
  - An example:
    - Organisation X asserts with a signed assertion in an Entity Attribute that entity Y was successfully audited according to a defined policy.
  - Asserting parties have to define a policy based on which it decides whether an entity is entitled for this assertion.
  - The reputation of such an assertion will decide on its usefulness.
    - Is metadata filtered using this criteria accepted by entities?

Summary

- Scalable Technical Trust can be achieved by Aggregators
  - Metadata Aggregators form the Metadata Layer, enabling scalable metadata exchange
- Scalable Behavioural Trust can be supported by defining policies which gain wide acceptance
  - Express adherence to a certain policy with an asserted tag
  - Metadata Tagging allows effective entity filtering
- Now we have to trial it and work on the details!