



Usage of SAML in eduGAIN

Stefan Winter, RESTENA Foundation
TERENA Networking Conference
Catania, May 16, 2006



Connect. Communicate. Collaborate

Outline

- eduGAIN overview and abstract operations
- SAML 1.1 overview
- Message flow
 - Requests and Responses
 - Finding the IdP
- Assertions
 - SAML assertions
 - shortcomings



Connect. Communicate. Collaborate

eduGAIN overview

- Goal: Connect existing identity federations
- Superstructure to transmit messages between federations
- Solves the problem of
 - Finding the federation to deal with
 - Message conversion
 - Ensuring trust between independent federations (in most cases: transitive trust)
 - Hiding most of the inter-federation superstructure to the federations involved
- Accessible via Java library



eduGAIN abstract operations

Connect. Communicate. Collaborate

- eduGAIN architecture document (DJ5.2.2) defines set of operations for four services
 - Authentication assertions
 - MetaData Service (p.k.a. Home Location Service)
 - Attribute release
 - Authorisation service
- Generic definition, can be mapped into multiple transport protocols
- SAML 1.1 is one of these protocols, SAML 2.0 will be another candidate later



Connect. Communicate. Collaborate

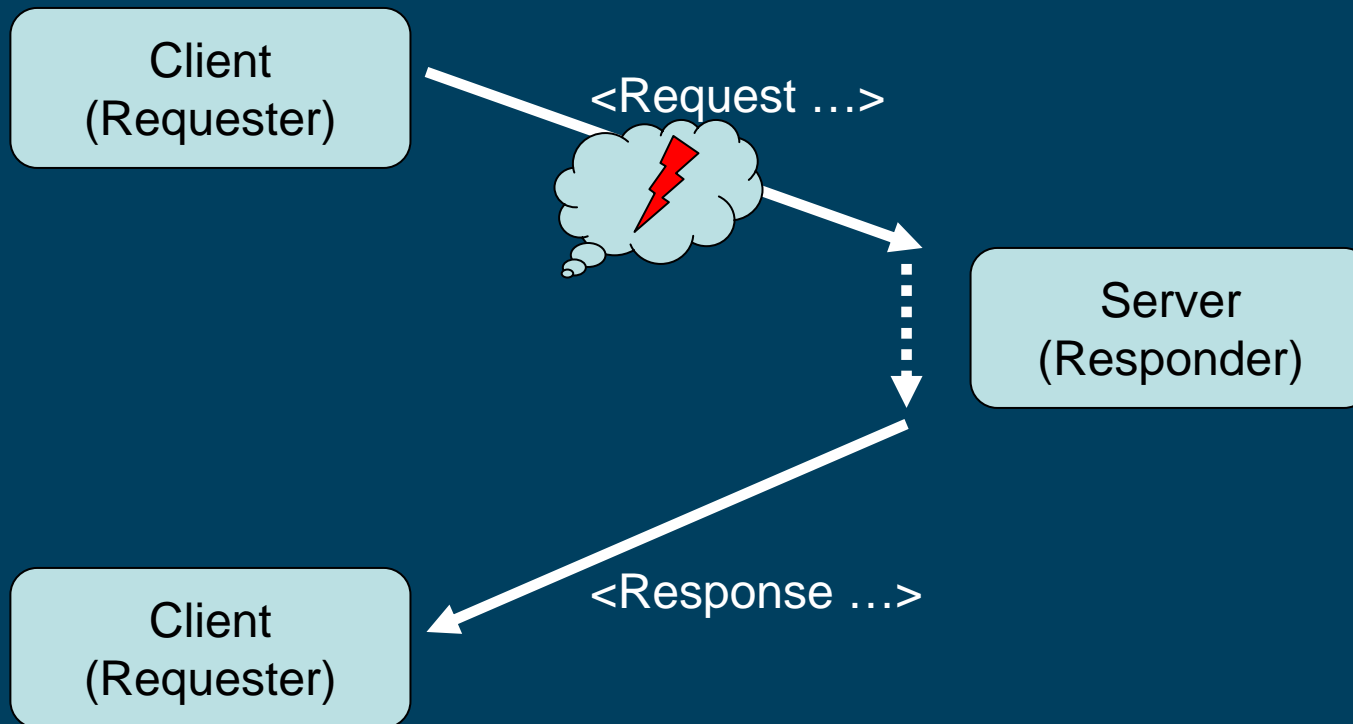
SAML 1.1 overview

- OASIS standard for authentication & authorisation
- XML Schemas for
 - SAML Protocol (exchange of SAML messages)
 - SAML Assertions (information about entities)
- Rules to use Schemas semantically correct
- Several types of information foreseen (“Assertions”)
 - Authentication assertions (not authentication)
 - Attribute assertions
 - Authorisation decisions
- Value of SAML lies in profile maps and implementation



Message flow

- Typical Client/Server protocol





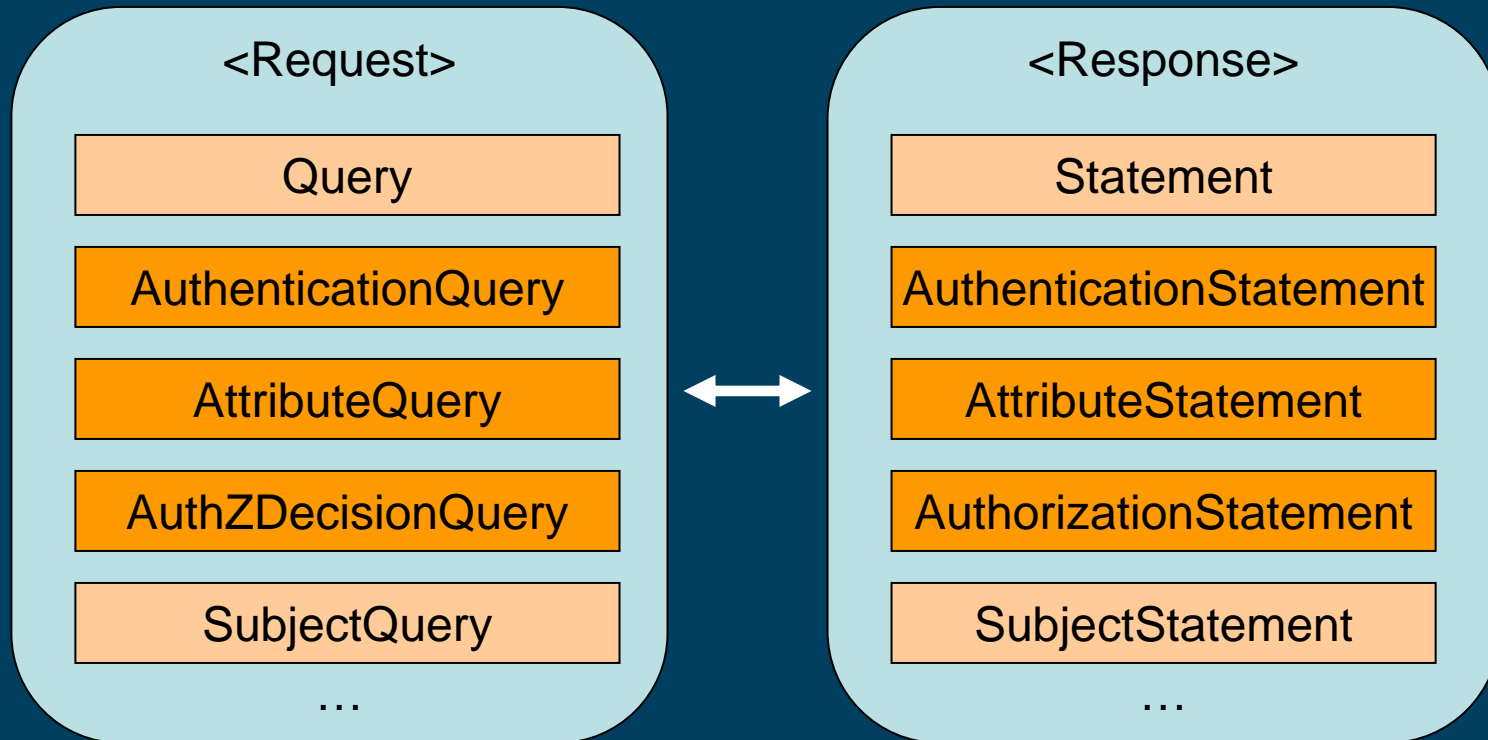
Connect. Communicate. Collaborate

Finding the IdP

- SAML 1.1 not prepared for federations: assumes that client knows the server
- No lookup service foreseen
- eduGAIN had two choices
 - Extend SAML schemas to include a MDS
 - Don't use SAML at all, find other means for finding the IdP
- SAML schema for original HLS was defined in DJ5.2.2, but for the moment, SAML is not used (HTTP REST instead)
- SAML 2.0 has its own means of transporting metadata



SAML Assertions



(darker parts used in eduGAIN)



Nuts and Bolts

Connect. Communicate. Collaborate

```
<samlp:Request RequestId="FooBar" MajorVersion="1" MinorVersion"1"  
  IssueInstant="2006-05-16 15:12">  
  <saml:AuthenticationQuery>  
    ...  
  </saml:AuthenticationQuery>  
  <saml:Signature>  
    0xdeadbeef  
  </saml:Signature>  
</samlp:Request>
```



Connect. Communicate. Collaborate

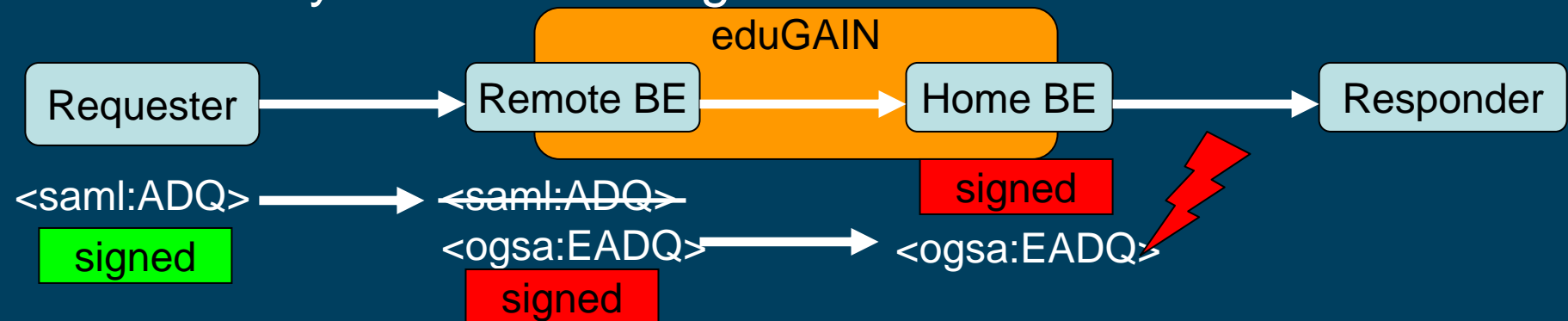
Limitations

- AuthenticationQuery
 - eduGAIN has optional parameter for actually performing authentication
 - SAML explicitly forbids transport of credentials
- Finding IdP not supported at all
- Trust: very often only transitive trust possible, no end-to-end (exception: Shib-to-Shib)
- <AuthorizationDecisionQuery>
 - eduGAIN can transport hints to the authorisation engine (e.g. for federations that do no attribute release and instead retrieve attributes during authorisation)
 - Not possible to convey in AuthZDecisionQuery



Limitations (2)

- Workaround: define `<ExtendedAuthZDecisionQuery>`, which can carry this piece of information (done by OGSA)
- Drawback: requires re-defining of SAML message parts up to `<Request>`
- Re-defining makes elements belong to a different namespace
- Possibly breaks XML signatures:





Connect. Communicate. Collaborate

The road ahead

- Why SAML 1.1?
 - When design decision was made, SAML 1.1 was largely deployed
 - SAML-based federations were using SAML 1.1 (esp. Shibboleth 1.3)
 - No decent publicly available implementation of SAML 2.0 available
- eduGAIN “v1” implementation based on SAML 1.1 underway
- Experiences gathered will be the base for later SAML 2.0 eduGAIN “v2”



Connect. Communicate. Collaborate

The road ahead - SAML 2.0

- SAML 2.0 supports metadata transport
 - Can be used for MDS
 - Parts already used in the non-SAML MDS transport
- Easier to extend than SAML 1.1
- openSAML2 current status: still in beta phase
- Authorisation part will probably not use built-in SAML constructs any more
 - Not flexible enough
 - Move to XACML officially recommended by OASIS

End



Connect. Communicate. Collaborate

Thanks for listening!

Questions?



Fondation RESTENA
Luxembourg