Security Token Service (STS) Update

Chad La Joie, SWITCH
(chad.lajoie@switch.ch)

MWSG Dec 7, 2007

www.eu-egee.org

Information Society and Media

Current State

- **Goal: Closer Shibboleth/Grid Integration**
- **Short-Lived Certificate Service**
  - Issue short-lived certificate based on SAML assertion from Shib
- **VOMS Attributes from Shibboleth**
  - SAML attribute, from Shib, available through VOMS in Attribute Certificate

Integration is non-disruptive, security still based on X.509 certificates.

Next Step

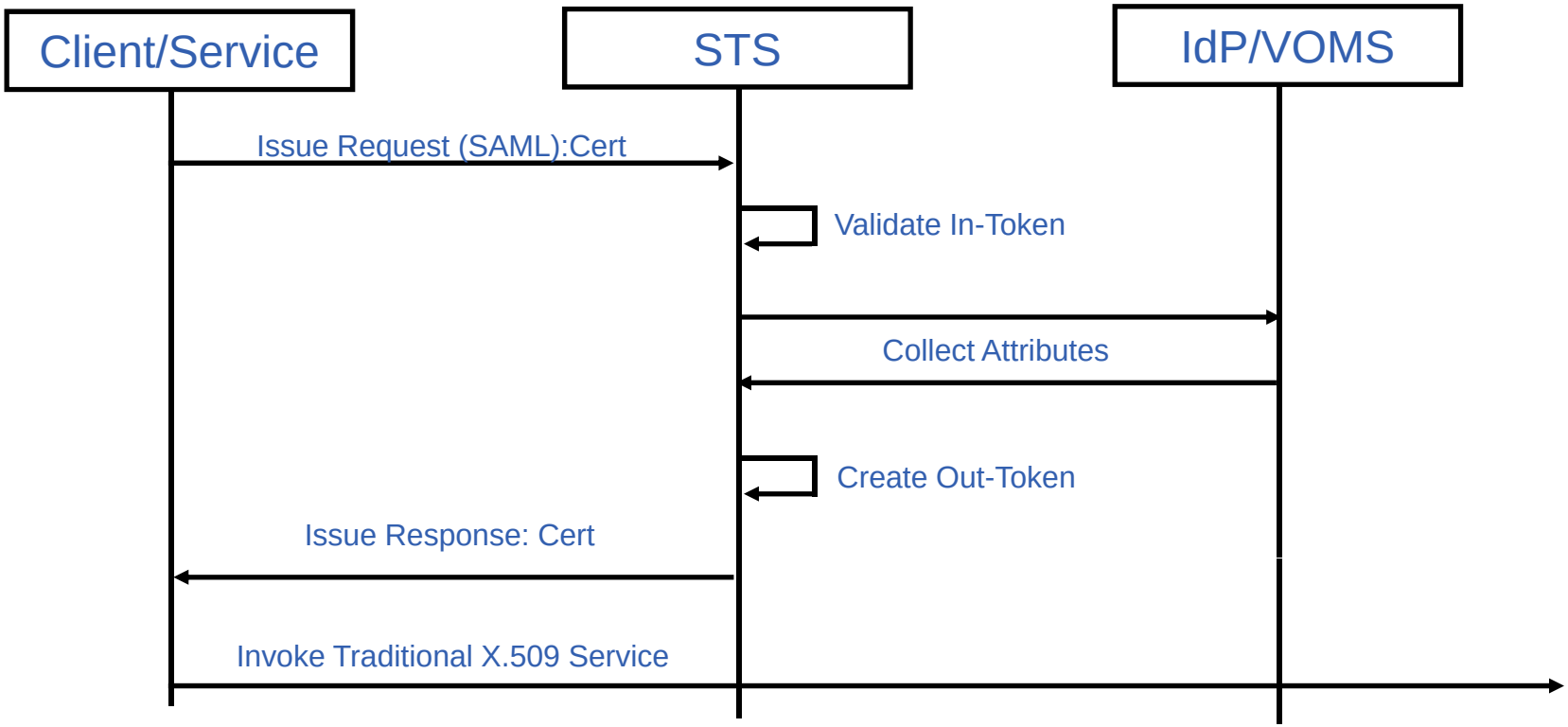
- **Goal: Allow use of SAML instead of X.509**
- **Problems:**
  - Can’t change every grid service from SAML to X.509 at once
  - Not all grid services are web services and can’t easily carry other security tokens
- **Other Issues:**
  - Client and services tied to token format
  - Client and services tied to proprietary protocols (proxy-init, voms-init); difficult to introduce new, but similar, services unless they support the existing protocol

Security Token Service

- **A service, based on WS-Trust, used to issue, renew, validate, and cancel security tokens**
- **Security Token: Any “thing”, carried within a message, used to identify a user to a service; X.509 cert, SAML assertion, Kerberos token, username/password**

- **Current Status**
  - Working draft of WS-Trust profile
  - Beginning of development of service built on Shibboleth 2 IDP framework
  - Beginning of developer of client built on Axis 2 framework and OpenSAML

What Does it Look Like



Benefits

- Can bootstrap client with local “home” credential
- Allows services to move to tokens as needed since client and services can transform tokens
- Policy-controlled token delegation, renewal, and attribute release
- Capable of supporting collection from multiple authorities
- Proprietary protocols hidden behind STS, if they need to change you can change them in one spot