# Security Token Service

## Transforming the Existing User Credentials for the Grid

Henri Mikkonen

Helsinki Institute of Physics

*ISGC 2012, 26.2.-2.3.2012*
*Academia Sinica, Taipei*

EMI is partially funded by the European Commission under Grant Agreement RI-261611

# Content

- Background
  - Requirements from the DCIs
  - EMI AAI Use Cases
- Security Token Service (STS)
  - Terminology
  - Functionality
- (Some) STS Use Cases



EMI INFSO-RI-261611

# Requirements from the DCIs

- *AAI needs of the DCIs* –workshop held at the EGI Technical Forum 9/2010
  - –Questionnaires for the projects crossing national boundaries and NGIs
- Participation & presentations from
  - –3 user communities
    - *Biomed, Earth Sciences, HEP*
  - –5 ESFRI projects
    - *CLARIN, Lifewatch, ELIXIR, EuroFEL, ILL*
  - –2 NGIs (Italy & U.K.)



EMI INFSO-RI-261611

# Highlights of the results

- Grid users do not want to handle multiple credentials
  - Users would like to obtain their Grid credentials using their existing user credentials
- DCIs would like to use federated identities
  - It is recognized that (inter)national federations are becoming more and more important
- X.509 certificates are and will be required by the majority of the Grid infrastructures for the foreseeable future

# EMI AAI WG's Use Cases

| Use case | Description | Current status |
|---|---|---|
| 1 | X.509 issuance based on AAI credentials | "Solved", but needs improvement |
| 2 | AAI-enabled portals to Grid infrastructures | Some solutions exist |
| 3 | AAI-enabled Grid information portals | Low priority |
| 4 | Security Token Service | New, general purpose service, high priority |
| 5 | Use of AAI attributes in the Grid | Interesting, potentially very important |
| 6 | Virtual Organization registration using AAI attributes | Low priority |

# Terminology

- Security Token?
  - « A collection of statements (claims) about a user or a resource »
    - *Anything that can be attached into a Web Service (SOAP) message*
    - *Example token formats: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password, …*
- Security Token Service?
  - « A Web service used to issue, renew, validate and cancel security tokens »



EMI INFSO-RI-261611

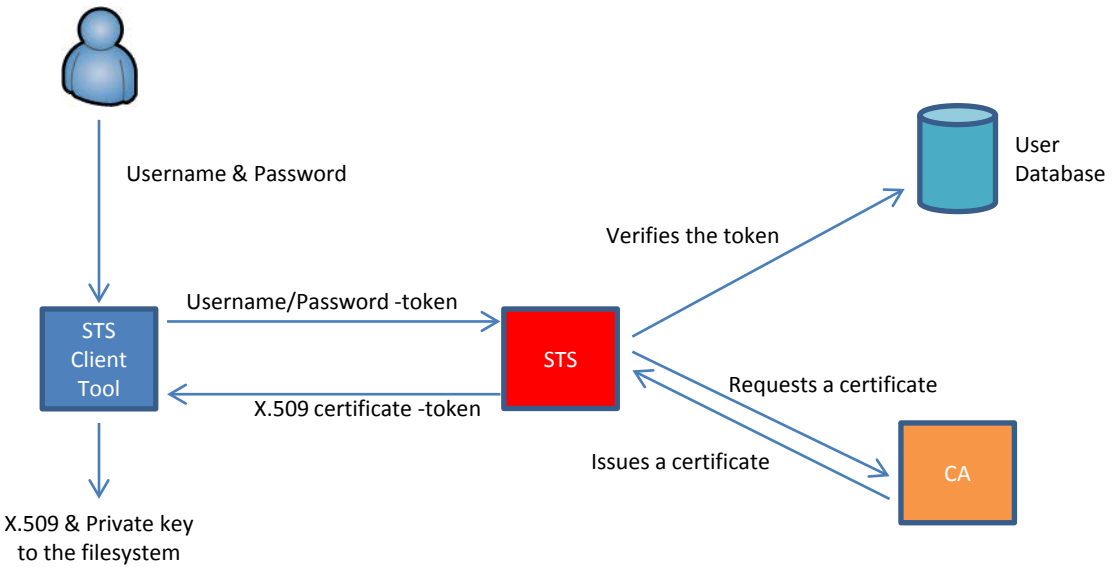
# STS ISSUE Functionality Overview

- Transforms the security token into another security token
  1. Validates the incoming security token
  2. Aggregates the required information & issues the new security token
     - *Possibly by exploiting external sources / authorities*
  3. Includes the new security token into the response message
- Establishes a trust relationship between different application domains



EMI INFSO-RI-261611

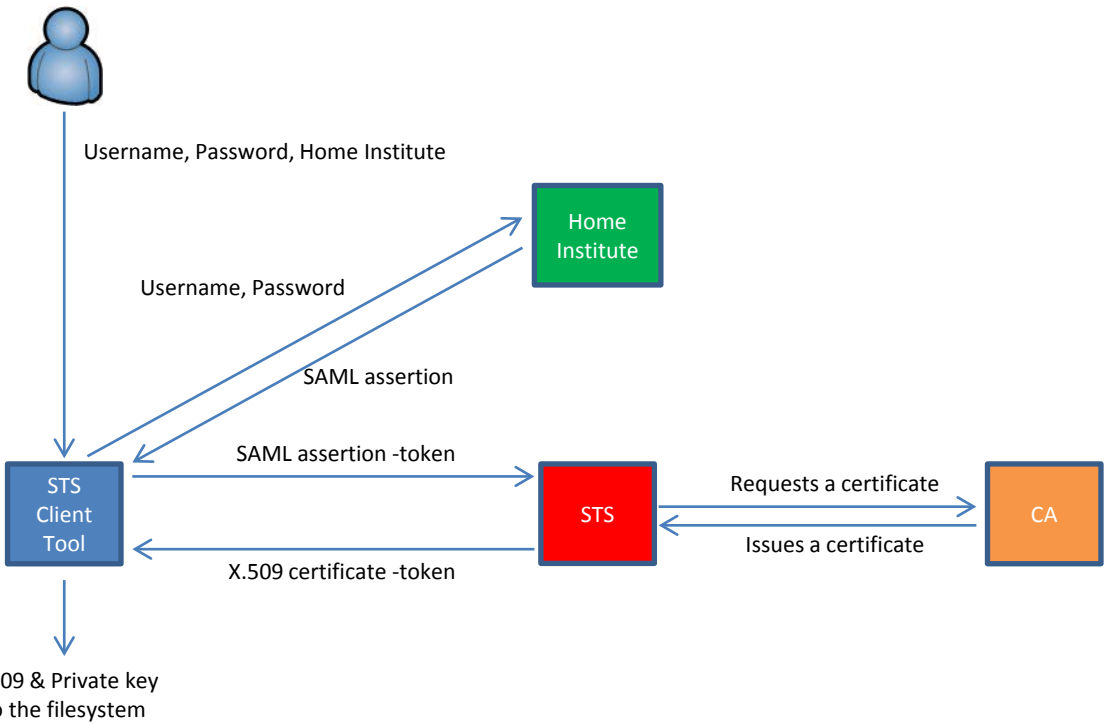
# Username/Password to X.509



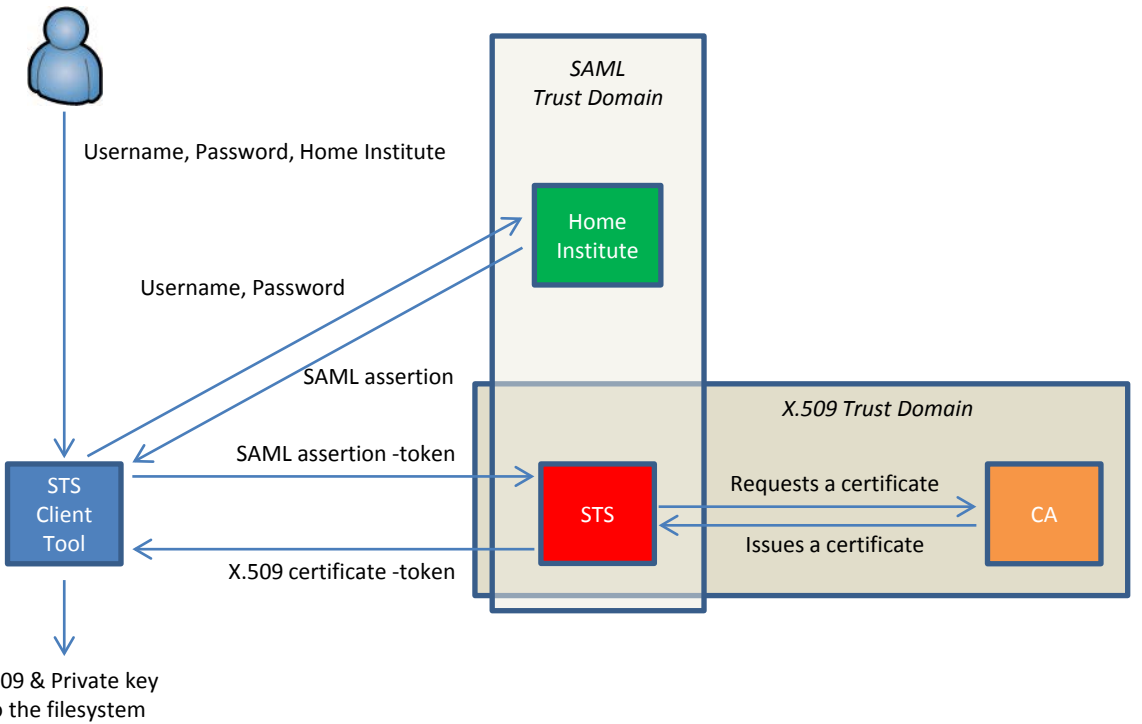



EMI INFSO-RI-261611

# SAML assertion to X.509



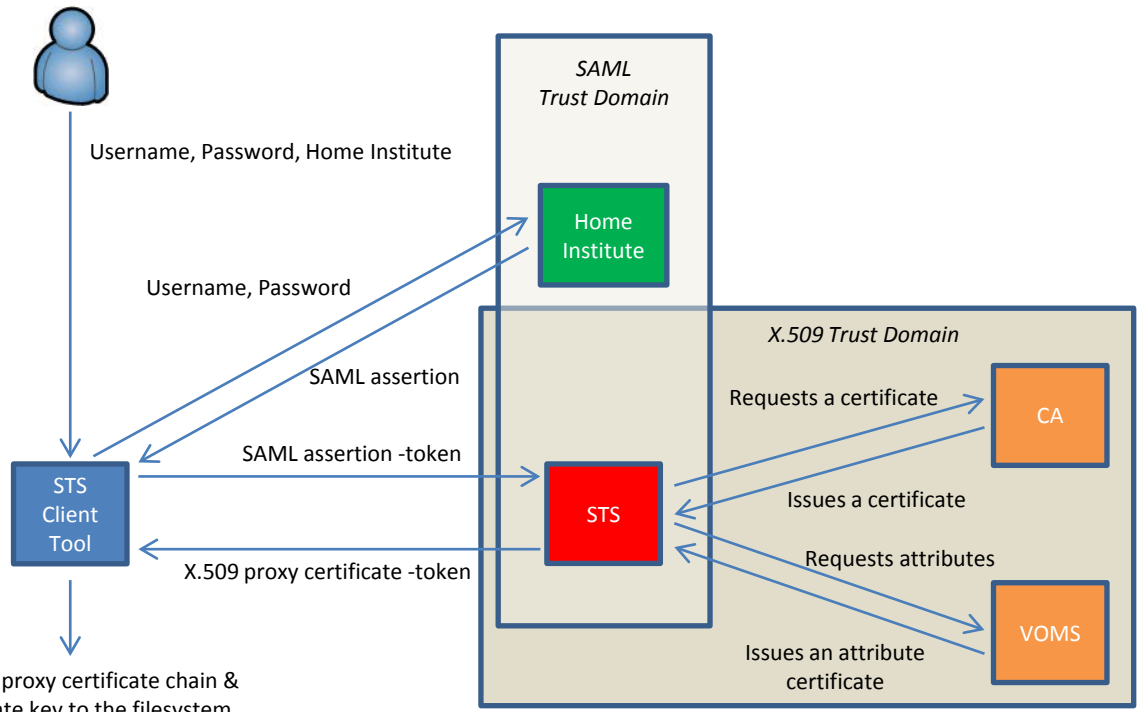
# SAML assertion to X.509






EMI INFSO-RI-261611

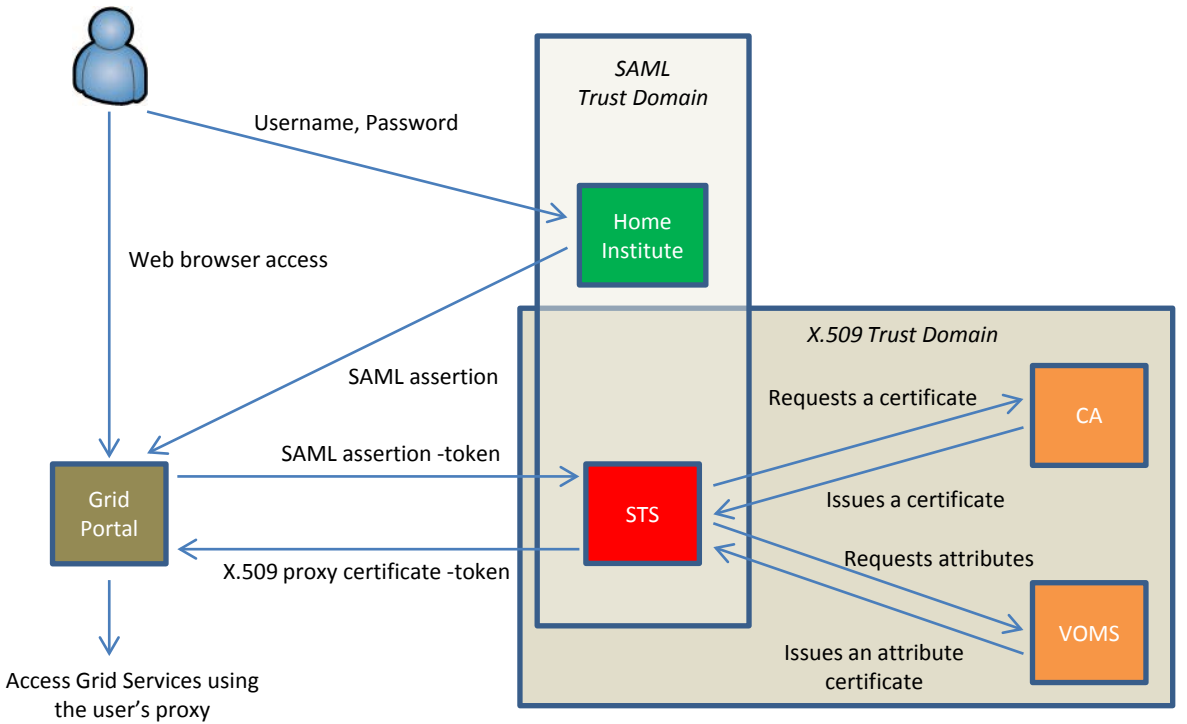
# SAML assertion to X.509 proxy






EMI INFSO-RI-261611

# SAML assertion to X.509 proxy






EMI INFSO-RI-261611

# Summary

- STS transforms an existing security token into another security token
  - Supported incoming formats: X.509, X.509 proxy, Username/Password, SAML, Kerberos
  - Supported outgoing formats: X.509, X.509 proxy, SAML
- STS is a SOAP-based Web Service
  - Any party capable of producing specified request messages and understanding response messages can act as a client
    - *Command-line clients, Web portals, Grid resources, …*

# Thank you! Questions?

Henri Mikkonen
<henri.mikkonen@cern.ch>

EMI is partially funded by the European Commission under Grant Agreement RI-261611