

Federated Grid Access Using EMI STS



Henri Mikkonen <henri.mikkonen@hip.fi>
Helsinki Institute of Physics (UH.HIP)

ISGC 2013, March 17-22, 2013
Academia Sinica, Taipei, Taiwan

- Problem definition
- Related work
- Security Token Service (STS) overview
- Use cases for federated identity
- (Short) Demonstration

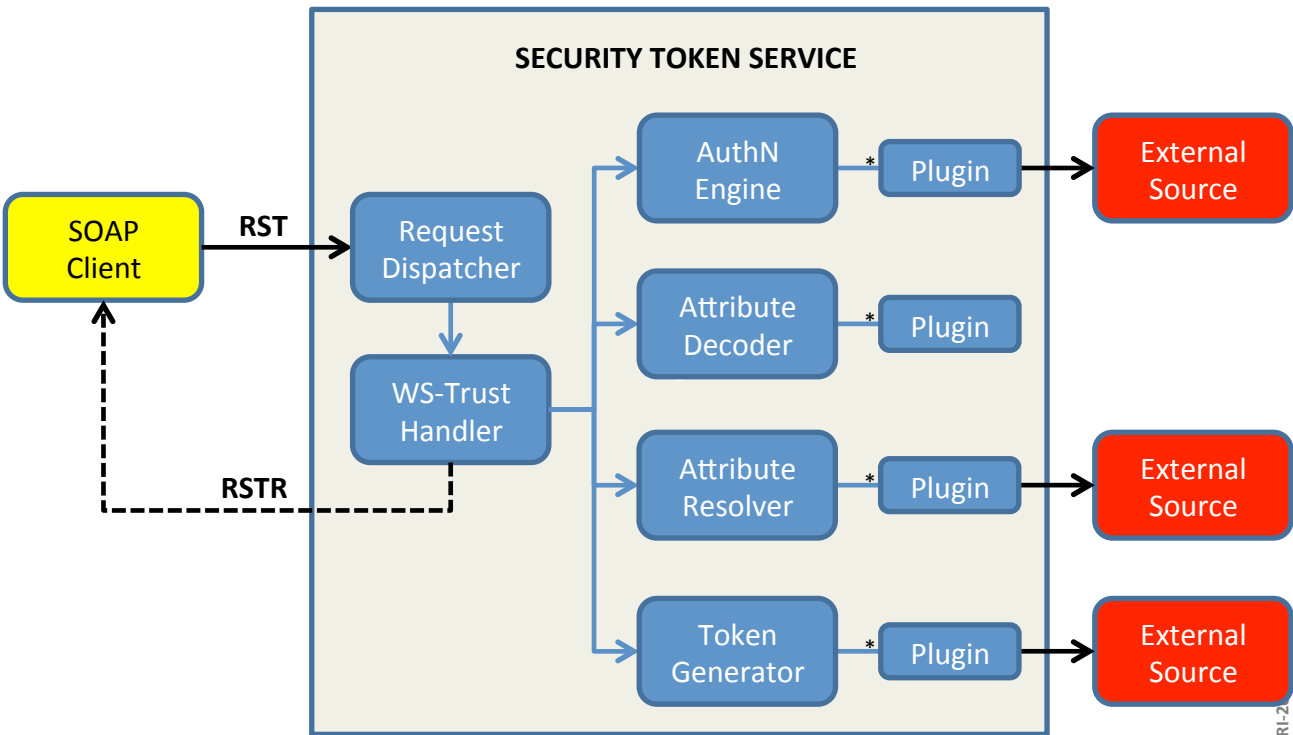
- Identity federations
 - National and international (eduGAIN)
 - De-facto standard is Security Assertion Markup Language (SAML)
 - Mostly Web-based
 - *Non-browser is coming up (e.g. Project Moonshot)*
- Grid middlewares
 - EMI: ARC, dCache, gLite and UNICORE
 - User authentication is based on X.509 certificates
 - Command-line and other non-browser clients

- Multiple solutions to X.509 issuance based on federated identity exist
 - Compatible IGTF profiles: Member Integrated Credential Services (MICS) and Short-Lived (SLCS)
- Most of them are at least partly Web-based
 - Either directly, or command-line client might be emulating a Web browser behind the scenes
- Proprietary protocols often used between the client and the service

- Grid identity is not just the X.509 certificate
 - gLite, ARC and dCache use *Grid proxies*
 - Grid proxy = End-Entity Certificate (EEC) + (short-lived) proxy certificate + private key
 - *Proxy certificate contains VO attributes*
- Grid proxy initialization (*voms-proxy-init*)
 - Request VO attributes from VOMS
 - Attach them into the proxy certificate which is signed by the private key corresponding to EEC
 - Default lifetime is 12 hours

- WS-Trust: *“STS is a Web service used to issue, renew, validate and cancel security tokens”*
 - Security Token: *“A collection of statements (claims) about a user or resource”* (WS-Security)
 - *Any digital identity that can be attached into a SOAP message*
 - STS establishes a trust relationship between different application / security domains
- EMI STS implements the ISSUE operation for the supported token formats

STS Architecture



- User knows username/password at his home institute & wants to access a Grid resource

Component	Credential input	Credential output
Grid resource	Grid Proxy	

- User knows username/password at his home institute & wants to access a Grid resource

Component	Credential input	Credential output
Grid resource	Grid Proxy	
VOMS	X.509 certificate	VOMS attributes

- User knows username/password at his home institute & wants to access a Grid resource

Component	Credential input	Credential output
Grid resource	Grid Proxy	
VOMS	X.509 certificate	VOMS attributes
Online CA	Certificate Signing Request (CSR)	X.509 certificate

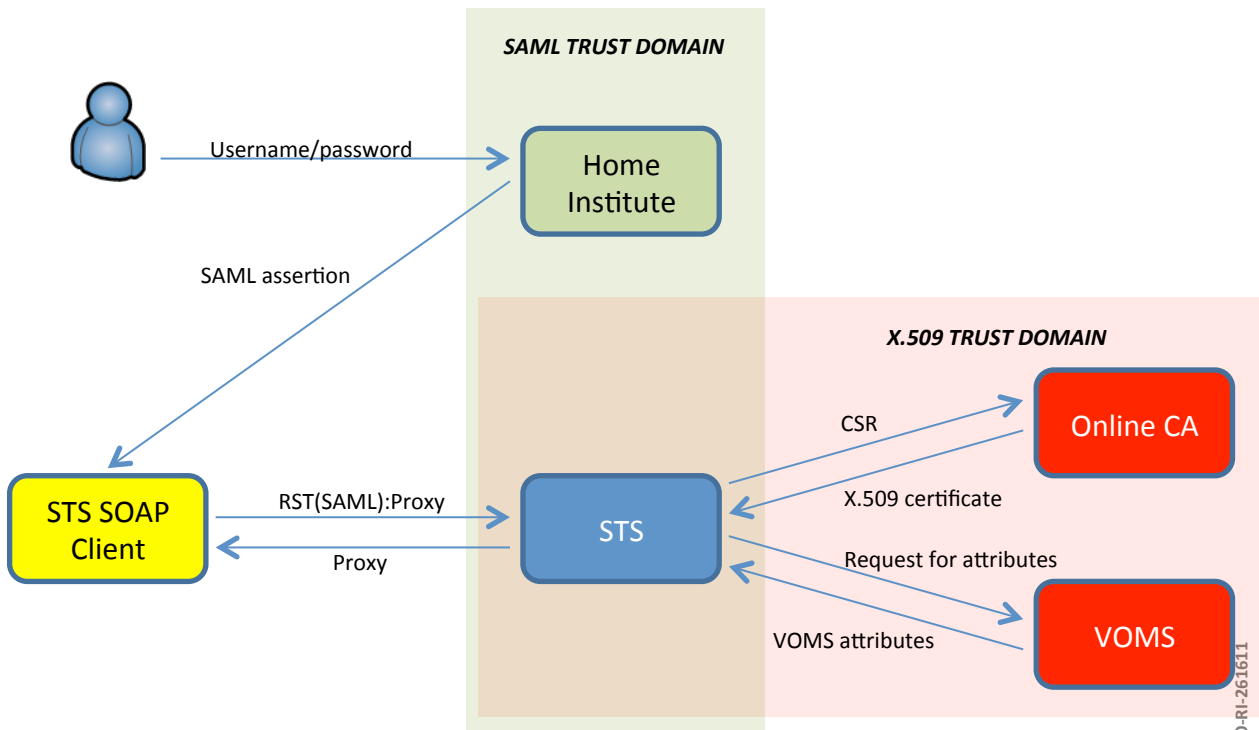
- User knows username/password at his home institute & wants to access a Grid resource

Component	Credential input	Credential output
Grid resource	Grid Proxy	
VOMS	X.509 certificate	VOMS attributes
Online CA	Certificate Signing Request (CSR)	X.509 certificate
STS	SAML assertion	Grid Proxy

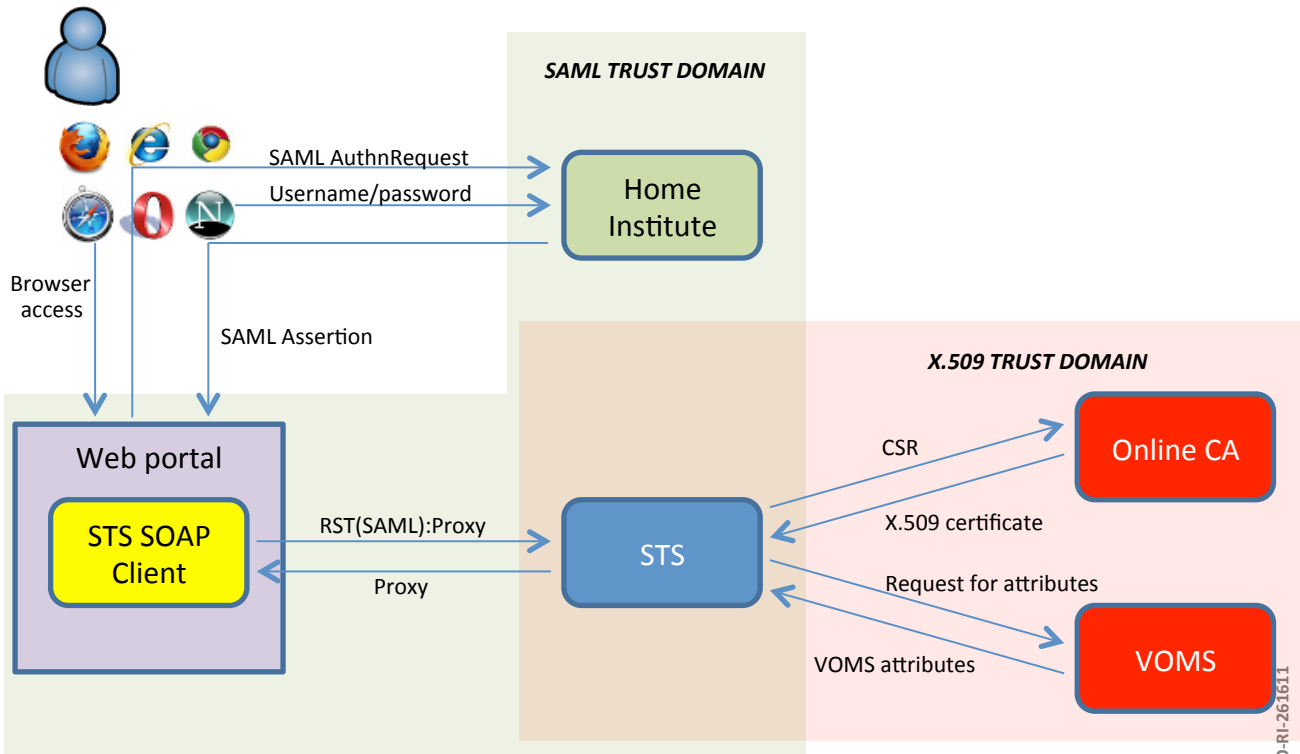
- User knows username/password at his home institute & wants to access a Grid resource

Component	Credential input	Credential output
Grid resource	Grid Proxy	
VOMS	X.509 certificate	VOMS attributes
Online CA	Certificate Signing Request (CSR)	X.509 certificate
STS	SAML assertion	Grid Proxy
Home Institute	Username/password	SAML assertion

SAML to Proxy - Components



Use case 1: Web portal



Use case 1: Web portal



SAML TRUST DOMAIN



- Relatively simple
- Uses SAML 2.0 Web SSO Profile
- Certificates nor private keys are never stored locally by the user



- Requires browser (to some users)
- If STS has different SAML entity than portal (as it should), SAML delegation is required

Browser access

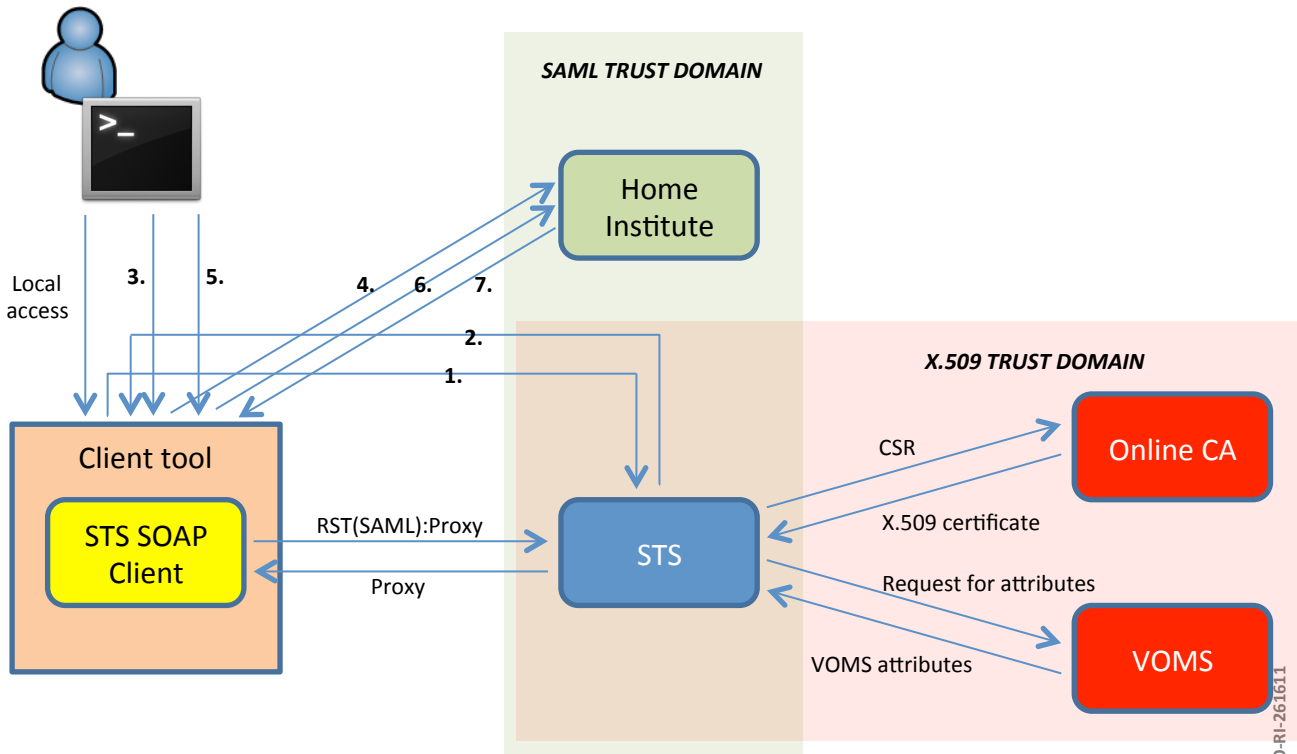
Web p

STS S
Clie

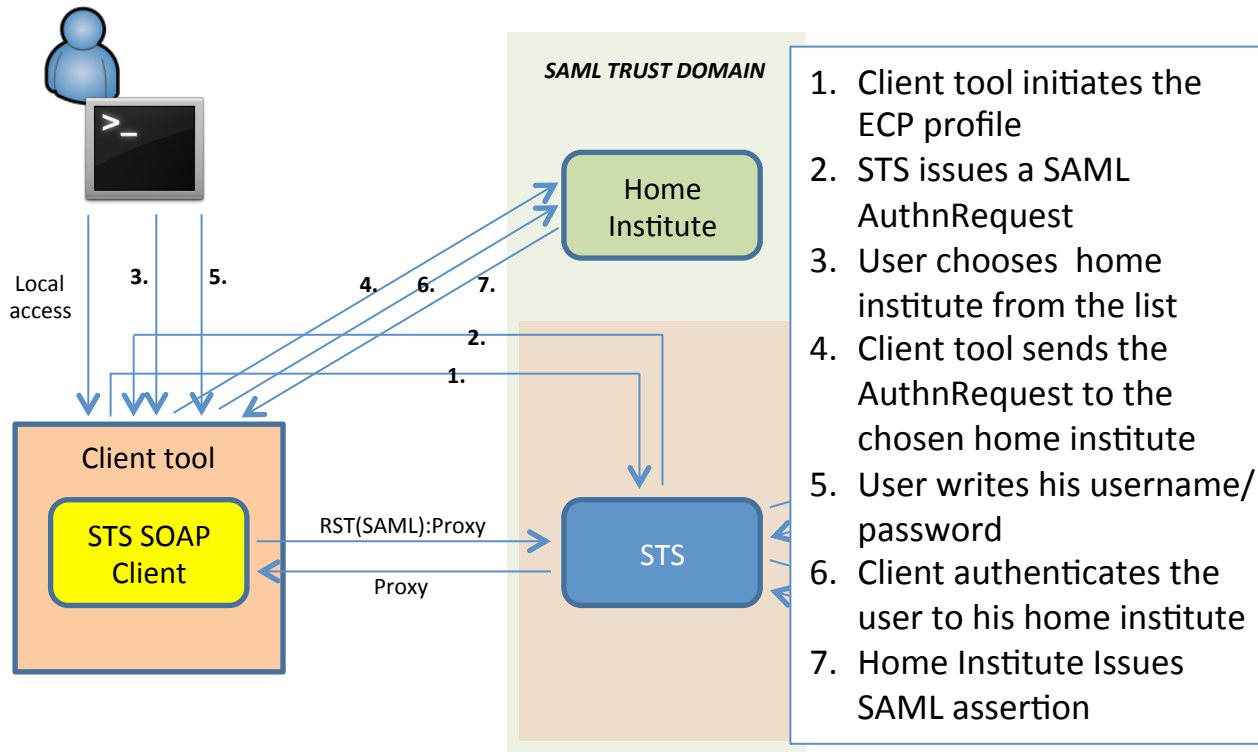
ine CA

OMS

Use case 2: CLI with ECP profile



Use case 2: CLI with ECP profile



Use case 2: CLI with ECP profile



SAML TRUST DOMAIN

1. Client tool initiates the



- No Web-browser required (to some users)
- Supported by Shibboleth Identity Provider (as of version 2.3)



- Not widely supported worldwide (a small fraction of the users need the ECP profile)

SAML assertion

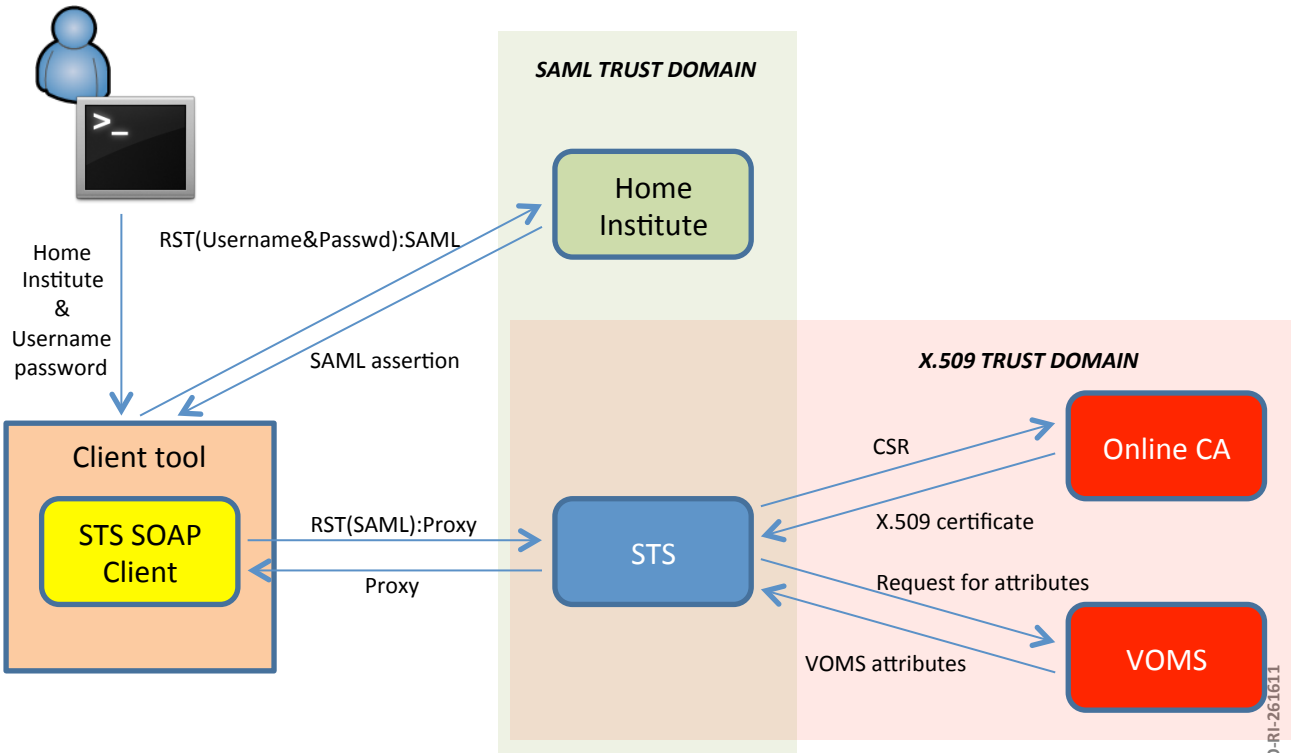
Local access

3.

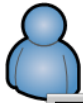
Client

STS S
Clie

Use case 3: CLI with another STS



Use case 3: CLI with another STS



Home
Institute
&
Username
password



Client

STS S
Clie

SAML TRUST DOMAIN



- Simpler than the ECP profile to be implemented



- Not widely supported by the open source SAML Identity Provider softwares

ine CA

OMS

- STS is a general purpose service used for transforming security tokens
 - It can be used in both Web browser and non-Web use cases for enabling Grid access using federated identity
 - SAML to X.509 & Grid proxy conversion
 - *Proxy initialization can be outsourced to STS*
- STS is relatively simple to be integrated
 - One SOAP message exchange between the client and the STS

Thank you!



STS is a part of the EMI-3 release:

<http://www.eu-emi.eu/emi-3-montebianco>

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