Technology programme,
http://tek.hip.fi

Exploring the SAML 2.0 ECP-Profile

Development of a client and a service provider prototype

Carolina Lindqvist
HIP summer student at CERN

carolina.lindqvist[at]cs.helsinki.fi

https://github.com/lindqvist/simple-ecp-client

Enhanced Client or Proxy (ECP)

The ECP Profile

The ECP-client and the Service Provider

Process flow

Messages

Demo

ECP Client

GET https://www.example.com/resource

Service Provider

Accept=text/html; application/vnd.paos+xml

PAOS=ver=”urn:liberty:paos:2003-08”; ”urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp”

Identity Provider

ECP Client

SP issues AuthnRequest

Service Provider

Identity Provider

SOAP Envelope

Headers:
PAOS Request
ECP Request

Body:
AuthnRequest

ECP Client

Service Provider

Client forwards AuthnRequest to IdP

SOAP Envelope

Headers:

Body:
AuthnRequest

Identity Provider

ECP Client

Service Provider

The IdP asks the client to identify themselves

Identity Provider

ECP Client

Service Provider

The client provides the IdP with a username and a password.

Identity Provider

ECP Client

Service Provider

If the authentication succeeds, the IdP sends a SAML Assertion to the client.

SOAP Envelope

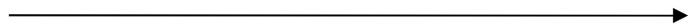
Headers:
ECP Response

Body:
Response

Identity Provider

ECP Client

The client forwards the SAML Assertion to the response consumer (SP).



Service Provider

SOAP Envelope

Headers:

Body:
Response

Identity Provider

ECP Client

The SP will register the client's login and redirect it to the initial resource.

Service Provider

Identity Provider

The SAML Assertion

Contains information about the authenticated user

```
<saml2:Attribute FriendlyName="cn" Name="urn:oid:2.5.4.3">
<saml2:AttributeValue xsi:type="xs:string">Tina Tester</saml2:AttributeValue>
```

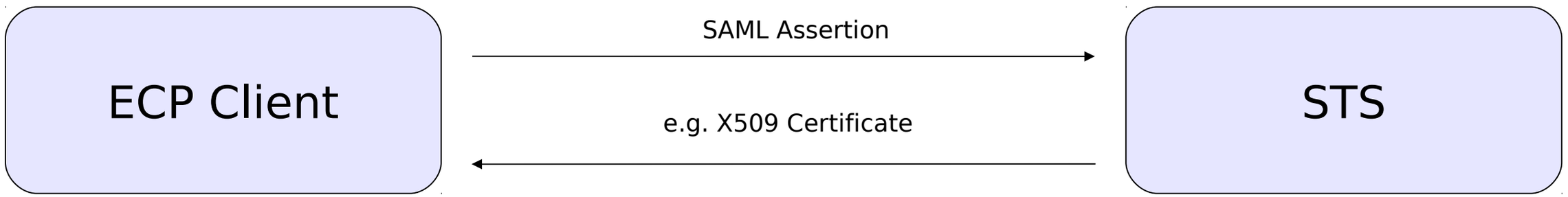
Simplifies authentication

Username + password

The assertion can be used with other services

STS, Hydra ...

Example: STS



Headers:
SAML Assertion

Body:
RequestSecurityToken
UseKey

Headers:
BinarySecurityToken

Body:
SecurityTokenResponseCollection

Demonstration :)

Questions?

ECP?

Assertion?

PAOS?