Step-up authentication and the art of creative SAML proxying

TNC2017
Pieter van der Meulen - SURFnet
Adding Step-up to a federation
Step-up when you’re a hub
Registration (1)

1\textsuperscript{st} factor + 2\textsuperscript{nd} factor = Self-Service

Tiqr
Registration (2)
Delegation of vetting
Service Architecture

Legend

- SAML Flow
- Network

Frontend

Backend
Event Sourcing

• Store all changes to the system in a “stream”

• A change is an “event” and contains all data relevant to the event

• Events are business: IdentityCreated, EmailVerified, SecondFactorVetted, ConfigurationUpdated

• You can reconstruct the state at any past moment in time, have full traceability and audit logs

• Store the “state” you need in projections
Step-up SAML proxy

1st factor
IdP

2nd factor

IdP

SP

IdP

SP

Step-up Proxy

AuthnRequest

Response
Transparant SAML Proxies

Proxy 1

Proxy 2

IdP

SP

IdP

SP

SP

IdP

Response

AuthnRequest

+ RequesterID

+ AuthenticatingAuthority

+ RequesterID

+ AuthenticatingAuthority

+ RequesterID

+ AuthenticatingAuthority
Trusted Proxy

- AuthnRequest
  - + RequesterID
  - + AuthenticatingAuthority

IdP

Response

SP

IdP

SP
Targeted IDs

IdP

SP

IdP

SP

Response

Subject

NameID

eduPersonTagetedID

NameID

Subject

AuthnRequest
Generic SAML Service Provider (GSSP)

1st factor
Response

2nd factor

Step-up Proxy

AuthnRequest
GSSP Registration

AuthnRequest

IdP

SP

Response

Subject

NameID
GSSP Authentication

GSSP Authentication

Subject
NameID

AuthnRequest

IdP

SP

Response

Subject
NameID
Second Factor Only (SFO) Authentication
Second Factor Only (SFO) Authentication
Second Factor Only (SFO) Authentication
More information and contact

- https://openconext.org/stepup/
- Pieter van der Meulen
  Pieter.vanderMeulen@surfnet.nl
  SURFnet