Configurazione SimpleSAMLphp

adesione ai profili di garanzia

Enrico Maria Vincenzo Fasanelli

Istituto Nazionale di Fisica Nucleare
(INFN)

Tutto in una slide (o quasi)

- L'INFN ha codificato i processi di verifica di ID e assegnazione LoA
- eduPersonAssurance con valori
  - **`urn:mace:infn.it:loa1`**
  - **`urn:mace:infn.it:loa2`**
- Corrispondenza netta con i profili IDEM
  - LoA1 → IDEM-P0
  - LoA2 → IDEM-P1
- SimpleSAMLphp ha una classe di «mapping» che fa al caso nostro
  - **`core:AttributeValueMap : Map attribute values to new values and attribute name.`**
- Mapping dei profili INFN in quelli IDEM e REFEDS in **`saml20-idp-hosted`**

```
'authproc' => array(
    10 => array(
        'class' => 'core:AttributeValueMap',
        'sourceattribute' => 'eduPersonAssurance',
        'targetattribute' => 'eduPersonAssurance',
        '%keep',
        'values' => [
            'https://refeds.org/assurance' => [
                'urn:mace:infn.it:loa1',
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/ID/unique' => [
                'urn:mace:infn.it:loa1',
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/ID/eppn-unique-no-reassign' => [
                'urn:mace:infn.it:loa1',
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/IAP/low' => [
                'urn:mace:infn.it:loa1',
                'urn:mace:infn.it:loa2'
            ],
            'https://idem.garr.it/af/IDEM-P0' => [
                'urn:mace:infn.it:loa1',
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/IAP/medium' => [
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/ATP/ePA-1m' => [
                'urn:mace:infn.it:loa2'
            ],
            'https://idem.garr.it/af/IDEM-P1' => [
                'urn:mace:infn.it:loa2'
            ],
            'https://refeds.org/assurance/profile/cappuccino ' => [
                'urn:mace:infn.it:loa2'
            ],
        ],
    ),
```

MFA

- Dal 31 ottobre è in produzione il sistema di autenticazione a doppio fattore (per adesso in fase pilota su un gruppo «ristretto» di power-users)
  - Basato su privacyIDEA Authentication System
  - Configurato solo per il personale staff (Dipendenti ed Associati)
  - Self-enrolment via autenticazione INFN-AAI con notifica a tutti gli indirizzi e-mail
  - Acquisizione del token registrata nel nostro Identity and Access Management System (GODiVA) e riportata in LDAP

    `schAcUserStatus: urn:schac:userStatus:it:infn.it:mfa:enabled`
  - Autenticazione con secondo fattore richiesta per l'accesso a tutti i SP INFN, via AuthProc nell'IdP SimpleSAMLphp, solo per chi ne è in possesso

MFA & IDEM-P2

- Secondo fattore solo per il personale staff (Dipendenti e Associati)
  - IAP/high
  - profile/espresso
- Non è garantito entro un giorno l'aggiornamento del valore di affiliazione per gli Associati (ma ci stiamo lavorando)
  - ATP/ePA-1m

Valori di eduPersonAssurance per IDEM-P2
https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign
https://refeds.org/assurance/IAP/low
https://refeds.org/assurance/IAP/medium
https://refeds.org/assurance/IAP/high
https://refeds.org/assurance/ATP/ePA-1m
https://refeds.org/assurance/ATP/ePA-1d*
https://idem.garr.it/af/IDEM-P0
https://idem.garr.it/af/IDEM-P1
https://idem.garr.it/af/IDEM-P2
https://refeds.org/profile/cappuccino
https://refeds.org/profile/espresso
* Opzionale

```
15 => array(
    'class' => 'core:AttributeValueMap',
    'sourceattribute' => 'schacUserStatus',
    'targetattribute' => 'eduPersonAssurance',
    '%keep',
    'values' => [
        'https://refeds.org/assurance' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/ID/unique' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/ID/eppn-unique-no-reassign' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/IAP/low' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/IAP/medium' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/IAP/high' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/ATP/ePA-1m' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://idem.garr.it/af/IDEM-P0' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://idem.garr.it/af/IDEM-P1' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://idem.garr.it/af/IDEM-P2' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/profile/cappuccino ' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
        'https://refeds.org/assurance/profile/espresso' => [
            'urn:schac:userStatus:it:infn.it:mfa:enabled'
        ],
    ],

),
```

AuthnContextClassRef (Non solo eduPersonAssurance)

- L'adesione ai profili di garanzia IDEM richiede che, oltre a eduPersonAssurance, venga opportunamente valorizzato –**in funzione della richiesta del SP-** anche l'atributo AuthnContextClassRef
- La risposta deve essere quindi calcolata in funzione di condizioni

• IDEM-P1

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere una delle classi seguenti:

- REFEDS SFA: https://refeds.org/profile/sfa
- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa

• IDEM-P2

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere la classe seguente:

- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/mfa

L’importanza della formazione

GARR

Configurazione SimpleSAMLphp
adesione ai profili di garanzia

cirrusgeneral (grazie ai nostri M&M)

- Modulo «coltellino svizzero» per SimplaSAMLphp
  - https://github.com/cirrusidentity/simplesamlphp-module-cirrusgeneral
- **ConditionalSetAuthnContext**
  - This AuthProc filter allows you to assert a specific authnContextClassRef if value in the users state equals some expected value. For example some upstream systems may indicate the user was required to perform MFA by setting an attribute on the user. This filter will allow you to assert https://refeds.org/profile/mfa if that attribute is present.
  - `schAcUserStatus: mfa:enabled` → https://refeds.org/profile/mfa
- **Conditional AuthProc Insertion**
  - There are use cases where you want to run a set of authproc filters, but only if a certain condition is met when a user is logging in. Not all authproc filters support conditional use. Subclasses of BaseConditionalAuthProcInserter allow you to insert an arbitrary number of authproc filters at the BaseConditionalAuthProcInserter priority during authproc processing. This allows you to check things in the user's state prior to creating the filters.
  - Se l'SP richiede https://refeds.org/profile/mfa allora eseguo il modulo privacyIDEA e definisco opportunamente il valore di AuthnContextClassRef

Grazie per
l’attenzione

www.garr.it/domande
codice: 2318 9129

Configurazione SimpleSAMLphp
adesione ai profili di garanzia