

Identifiers in SURFconext

WHAT'S NEXT AT SURFCONEXT 2018



- Bart Geesink - SURFnet

Wat is een identifier in de context van SURFconext?

- Een “string” die een gebruiker identificeert
 - Bijvoorbeeld:
 - geesink@surfnet.nl
 - 2f2d5ed231d2c276f5f36209332e3d5c1c0f8954
 - urn:collab:person:surfnet.nl:geesink

NamID's

- In SAML wordt het “NameID” element gebruikt om een gebruiker te identificeren
- SURFconext overschrijft de NameID van de IdP
- Er zijn twee types “NameID” binnen SURFconext :
 - **Persistent nameID**
 - **Transient nameID**

Transient nameID

- Ziet er zo uit: ***01ae7bf92ab272e1213c09c4e40fd8f63c148253***
- Is elke sessie anders (en dus eigenlijk geen identifier)
- Wordt toegepast als het niet nodig is om terugkerende gebruiker te identificeren
- De meest privacy vriendelijke “identifier”

Persistent nameID

- ziet er zo uit: **2f2d5ed231d2c276f5f36209332e3d5c1c0f8954**
- Uniek *per SP*
- Blijft altijd gelijk
- Lekt geen persoonsgegevens
- Wordt door SURFconext gegenereerd:
 - Wordt gegenereerd uit: “uid” (aangeleverd door IdP) + “SP entityID” + “SchacHomeOrganisation” + “secret”

Identificerende attributen

- Sommige attributen kunnen worden gebruikt om een gebruiker verder te identificeren
- Bijvoorbeeld handig wanneer:
 - Een applicatie migreert naar SURFconext en al een bestaande identifier heeft
 - Koppelen van gegevens tussen applicaties
 - Identifier wordt ook op andere plekken gebruikt

eduPersonTargetedID

- Kopie van het nameID in een attribuut
- Kan worden gebruikt in software die geen identifier uit het nameID kan halen

```
</ds:Signature>
<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">195aa888e663f4e7f7728839e2a63689de88fcb9</saml:NameID>
</saml:Subject>
<saml:AttributeStatement>
  <saml:Attribute Name="urn:mace:dir:attribute-def:eduPersonTargetedID"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    <saml:AttributeValue>
      <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">195aa888e663f4e7f7728839e2a63689de88fcb9</saml:NameID>
    </saml:AttributeValue>
  </saml:AttributeStatement>
```



The diagram consists of two arrows. One arrow points from the text 'Kan worden gebruikt in software die geen identifier uit het nameID kan halen' to the first NameID value in the XML snippet. The second arrow points from the second NameID value (located inside the AttributeStatement) back to the first NameID value, illustrating that the attribute contains a copy of the subject's NameID.

schacPersonalUniqueCode (student of medewerker nummer)

- Student of medewerkernummer geleverd door de IdP
- Heeft deze vorm:
 - urn:schac:personalUniqueCode:nl:local:example.edu:employeeid:**x12-3456**
 - urn:schac:personalUniqueCode:nl:local:example.nl:studentid:**s1234567**
- urn:schac:personalUniqueCode:nl:local: Wordt door SURFnet beheerd, registratie kan bij SURFnet worden aangevraagd
- Kan meer dan een waarde bevatten (multi-valued)
- Wordt vooral gebruikt om accounts te matchen met interne applicaties

eduPersonPrincipalName

- Unieke identifier voor een gebruiker in de vorm [user@domain](#)
- Wordt geleverd door de IdP
- Het domein is eigendom van de IdP
- Lijkt op een emailadres, maar is het niet (vergelijk UPN in Microsoft land)

- UID zoals geleverd door de IdP (“gebruikersnaam”)
- Uniek *binnen* een instelling, maar niet tussen instellingen (bijvoorbeeld de uid 'bart')

Mail (gebruik maar liever niet)

- e-mail adres zoals geleverd door de IdP
- Kan multi-valued zijn
- Ongeschikt als identifier:
 - Kan over tijd wijzigen (geesink@surfnet.nl wordt geesink-jansen@surfnet.nl bij huwelijk bijvoorbeeld)
 - Multi value kan problemen opleveren
 - Kan opnieuw worden toegewezen als iemand uit dienst is



- Relatief nieuw attribuut
- Uniek nummer gebruikt om wetenschappelijke auteurs te kunnen onderscheiden (zie <https://www.orcid.org>)
- Kan worden gekoppeld met een SURFconext account en vervolgens worden meegegeven in een attribuut
- Heeft de vorm van een URL: “**<https://orcid.org/0000-0002-4926-2859>**”

Vragen?

- Ervaringen met identifiers?
- Ontbreekt er wat aan SURFconext?