TCS SAML demo background

https://www.digicert.com/sso

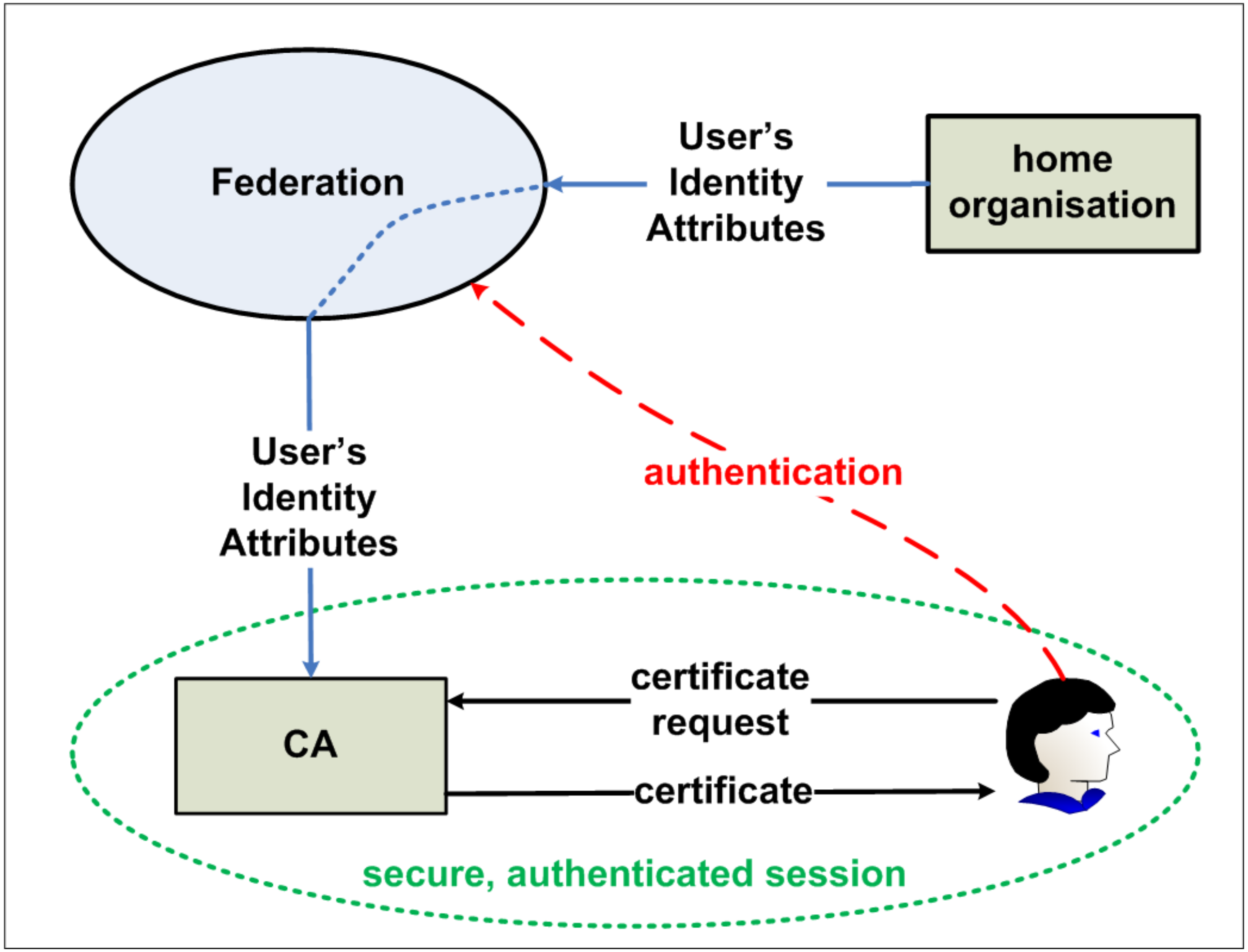
David Groep

TCS PMA and Nikhef

TCS TNC2015 Workshop

June 16, 2015

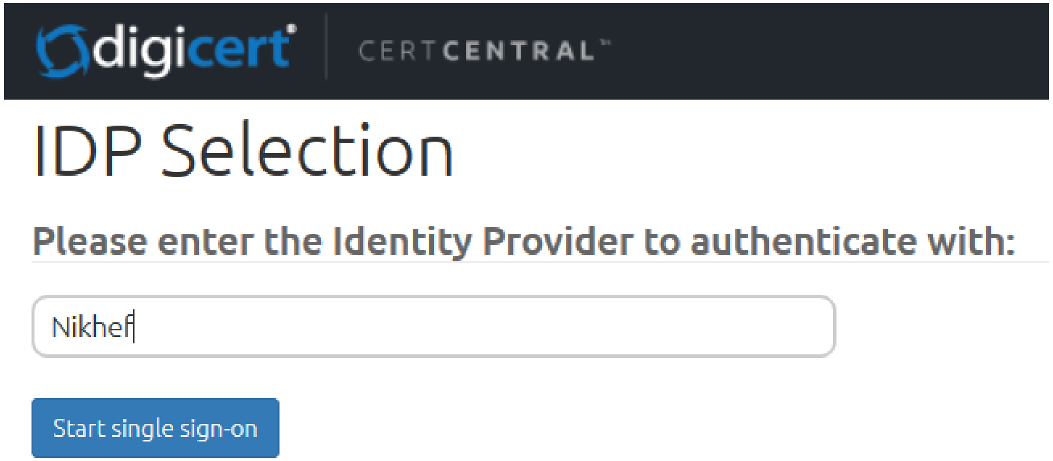
SAML Issuance via the DigiCert SSO portal


Federation
User's Identity Attributes
home organisation
authentication
User's Identity Attributes
certificate request
CA
certificate
secure, authenticated session

Graphic courtesy Jan Meijer, Uninett, 2009(!)

SSO SAML portal now natively hosted by DigiCert

- Scope: **client certificates** (and client certificates only, sorry!)
- We no longer need a intermediary portal such as Djangora
- DigiCert itself is a SAML2Int Service Provider
  <md:EntityDescriptor entityID="https://www.digicert.com/sso">
- visible to Federations and IdPs via the eduGAIN meta-data
- DigiCert will know about all IdPs in eduGAIN (via eduID.at)



IDP Selection

Please enter the Identity Provider to authenticate with:

Nikhef

Supported products

Supported products

- **Client Premium** – email signing and authentication
- **Grid Premium** – authentication with guaranteed unique subject name (DN)
- **Grid Robot Name** – authentication for M2M communication

Intentionally unsupported client products

- Email Security Plus – *this is a key-escrowing product that is only useful for managed deployment, is potentially dangerous, and the escrow isn't available anyway …*
- Digital Signature Plus – *this is just a dumbed down version of Premium*
- Grid Robot Email – *the product has additional policy requirements that are unlikely to be satisfied by arbitrary users*
- Grid Robot FQDN – *the product additional requires DCV-like validation that cannot be done at the user level*

How to get the SAML SSO service enabled

Who can get client certs via Federated SSO? Users of all IdPs that are

- part of an subscriber that has signed up to TCS via their NREN
- have their IdP data published in the eduGAIN meta-data
  are you ready? look for your own entityID in http://mds.edugain.org/ … like
  <md:EntityDescriptor entityID="https://sso.nikhef.nl/sso/">
- where the subscriber has
  - registered and validated at least one organisation, and has
  - a SAML2Int IdP that releases schacHomeOrganisation, and that is
  - linked to that organisation via the CertCentral portal by an admin
- and the requesting user has the proper eduPersonEntitlement

Important changes compared to the ‘2009-series TCS’

- there is **no sematic difference** between ‘personal’ and ‘e-science’ anymore!
  *i.e. whichever of the two entitlement you have, you can order all products since the validation requirements are **exactly the same** anyway!*
- eScience robot machine-to-machine user-named certificates available now

Attributes that should come from the IdP

In order to link the IdP to a specific organisiation

… *remember: one or more organisations are part of a single Division*

- *schacHomeOrganisation* – verified by the federation, please…

Release the usual attributes about the requester ('same' as for previous TCS):

- Basically release the "Research & Scholarship" attribute set
- For eligible entities should be 'true' values as required by the TCS G3 CPS
- *displayName* – reasonable representation of the **real name**,
  i.e. it should not be user-modifiable without validation
  if absent: *commonName*, if absent: *givenName*+" "+*sn*
- *mail* (e-mail address) – a (single for now) verified address **from the IdM**
- *eduPersonEntitlement* to define (a subset of) eligible requesters in IdM
  `urn:mace:terena.org:tcs:personal-user`
  `urn:mace:terena.org:tcs:escience-user`

Now for the real demo

- http://www.digicert.com/sso (for requesters)

- https://www.digicert.com/secure/saml/org-map/ (for Org-Division admins)

In due time (by July 1st)

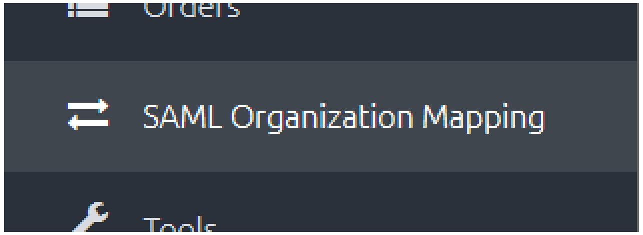
- https://tcs-escience-portal.terena.org/
- https://tcs-personal-portal.terena.org/

will start to contain text that informs users about the new service location

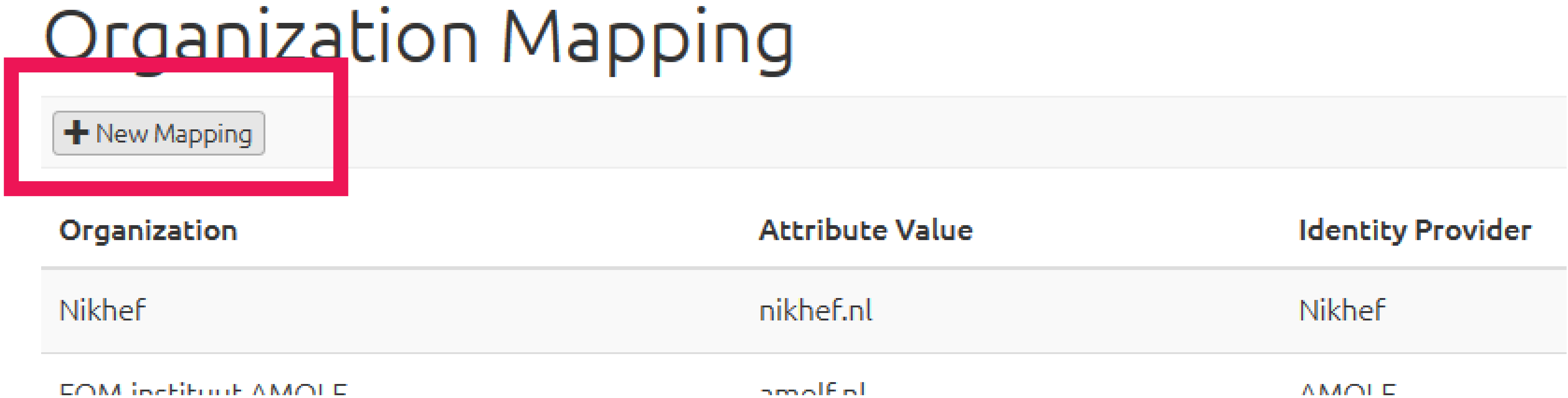
- the actual URLs will remain (since external things link to it)
- If you have your own custom URLs, these should be pointed to a server that hosts a similar page (or does a HTTP redirect to the above URL)

Link your organisation to your IdP in CertCentral

- First of all, login to CertCentral with an Administrator account, and assign “SAML Administator” right to yourself
- Then click “SAML Organisation Mapping”



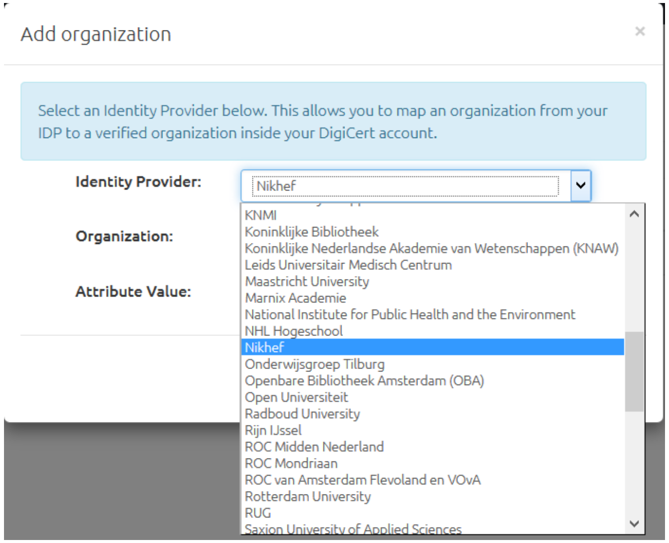
- Then create a new mapping



Organization	Attribute Value	Identity Provider
Nikhef	nikhef.nl	Nikhef
FOM instituut AMOLF	amolf.nl	AMOLF

Setting schacHomeOrganization

- Seect your IdP from the list – this list comes from the eduGAIN meta-data, and the subset is the set of entities for whom your NREN is the registrar



Add organization

Select an Identity Provider below. This allows you to map an organization from your IDP to a verified organization inside your DigiCert account.

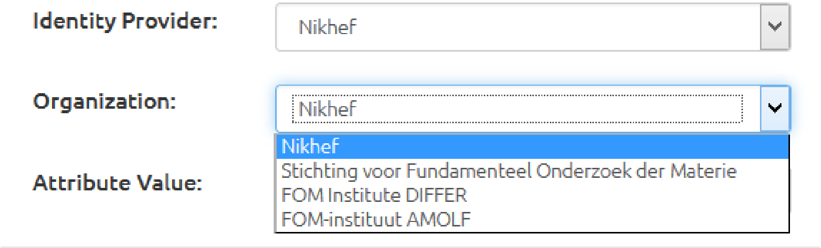
Identity Provider: Nikhef

Organization:

Attribute Value:

×
KNMI
Koninklijke Bibliotheek
Koninklijke Nederlandse Akademie van Wetenschappen (KNAW)
Leids Universitair Medisch Centrum
Maastricht University
Marnix Academie
National Institute for Public Health and the Environment
NHL Hogeschool
Nikhef
Onderwijsgroep Tilburg
Openbare Bibliotheek Amsterdam (OBA)
Open Universiteit
Radboud University
Rijn IJssel
ROC Midden Nederland
ROC Mondriaan
ROC van Amsterdam Flevoland en VOvA
Rotterdam University
RUG
Saxion University of Applied Sciences

- Now select the validated organisation to which this IdP should be linked

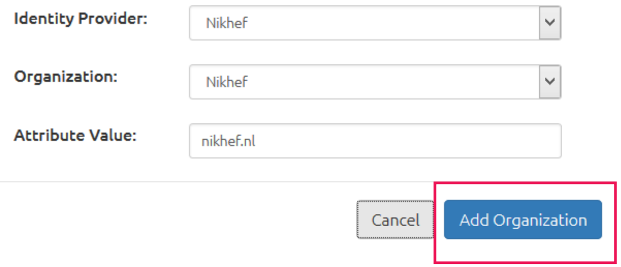


Identity Provider: Nikhef

Organization: Nikhef

Attribute Value:

- And specify what the value for schacHomeOrganization will be for users that are to be mapped from this IdP to this organisation – and click “Add Organisation”



Identity Provider: Nikhef

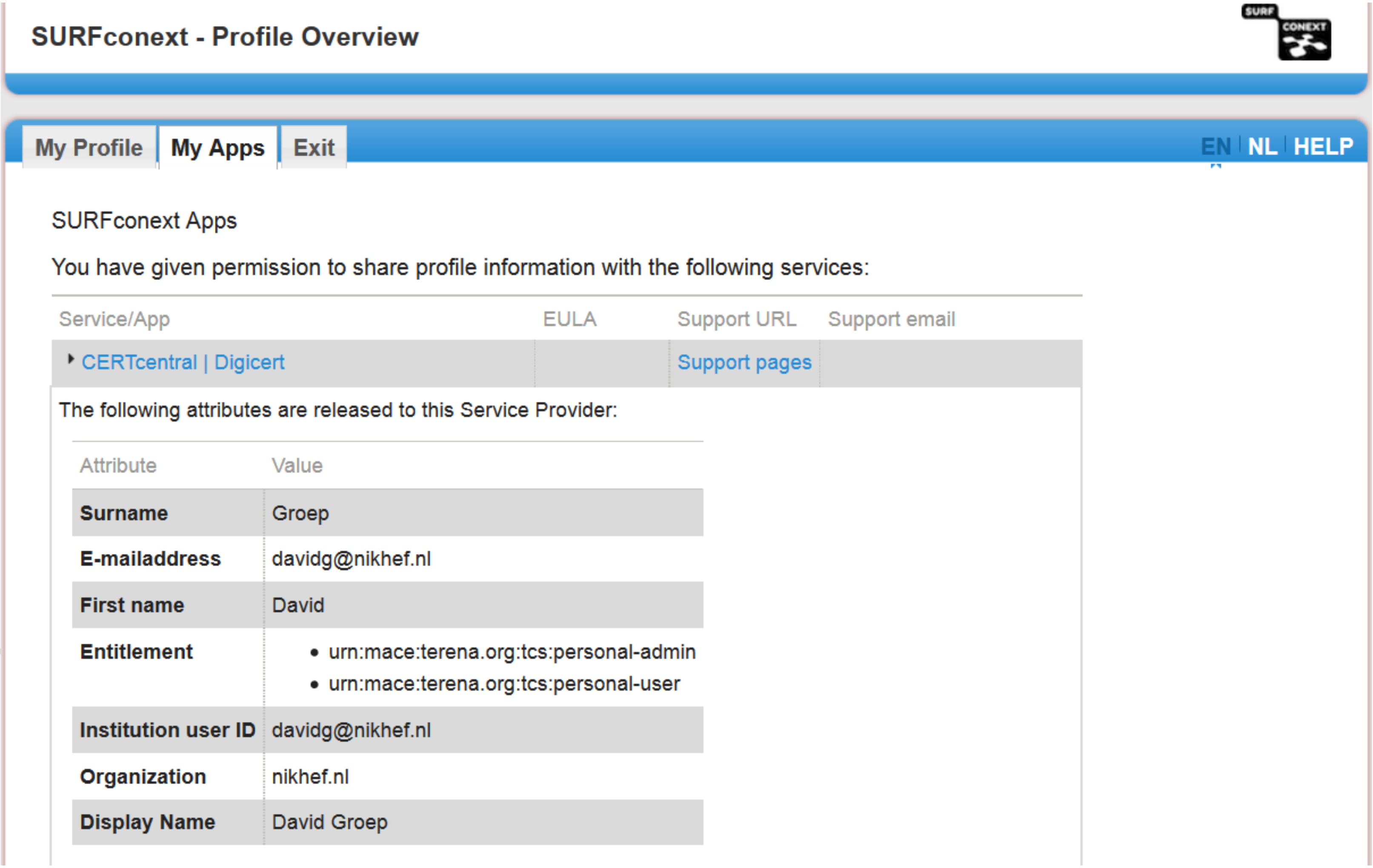
Organization: Nikhef

Attribute Value: nikhef.nl

Testing the link

- Users logging in to https://www.digicert.com/sso should now see their IdP
- When logging in, the Organisation is set to the right value
- Common name &c is taken from the SAML attributes

Attributes released (for me …)



SURFconext Apps

You have given permission to share profile information with the following services:

Service/App	EULA	Support URL	Support email
CERTcentral | Digicert		Support pages	

The following attributes are released to this Service Provider:

Attribute	Value
Surname	Groep
E-mailaddress	davidg@nikhef.nl
First name	David
Entitlement	• urn:mace:terena.org:tcs:personal-admin • urn:mace:terena.org:tcs:personal-user
Institution user ID	davidg@nikhef.nl
Organization	nikhef.nl
Display Name	David Groep

CSR based requests

- Example CSR, manually generated via any tool, e.g.

```
openssl req -new -keyout tcsg3-demo-davidg-20150616.key
    -out tcsg3-demo-davidg-20150616.req -subj '/CN=davidg'
```

- The result will be **sent back by email** immediately
- Login again (sorry) to see it in your list of orders and download on-line

Conversion commands

- Convert browser-exported PKCS#12 to combined PEM cert+key file

```
openssl pkcs12 -in tcsg3-demo-davidg-20150616.p12 -out
tcsg3-demo-davidg-20150616.crt+key
```

- Just the public cert

```
openssl pkcs12 -in tcsg3-demo-davidg-20150616.p12 -
nokeys -out tcsg3-demo-davidg-20150616.crt
```

- Convert key and cert file to PKCS#12

```
openssl pkcs12 -export -name “TCSG3 Premium Client David
Groep” -keyin tcsg3-demo-davidg-20150616.key -in
david_groep_davidg_nikhef_nl/david_groep_davidg_nikhef_n
l.crt -out tcsg3-demo-davidg-20150616.p12
```

- Just show a PKCS#12 file

```
openssl pkcs12 -in tcsg3-demo-davidg-20150616.p12 -info
-nokeys
```

Thank you

https://www.digicert.com/**sso**

davidg@nikhef.nl

GÉANT

Networks · Services · People
www.geant.org