Persoonlijke Certificaten via SURFconext

- DigiCert heeft één gecombineerde portal om via SURFconext Single Signon zowel normale als eScience Grid persoonlijke certificaten te bestellen: **https://www.digicert.com/sso**

- Via SURFconext stuurt de Identity Provider (IdP) van een SURFcertificaten deelnemer attributen naar DigiCert en die geeft persoonscertificaten terug. Iemand die met zijn correcte naam in de IdP is opgenomen kan zo een certificaat krijgen *zonder* een username/password te hebben in www.digicert.com. In de IdP moet een gebruiker wel de entitlement (bevoegdheid) van zijn instelling hebben gekregen om certificaten te krijgen. Als "My Profile"/"Mijn Profiel" in het profile van een gebruiker niet urn:mace:terena.org:tcs:personal-user (of urn:mace:terena.org:tcs:escience-user) bevat kan hij geen certificaat bestellen.

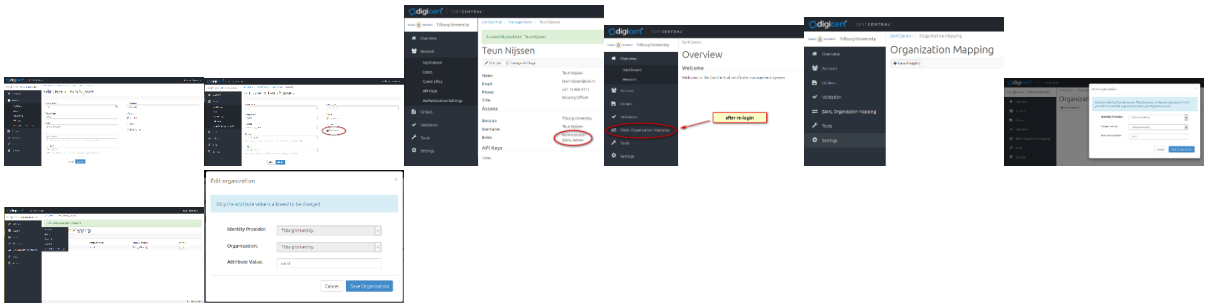
- DigiCert gebruikt eduGAIN - Géant als lijst van toelaatbare IdP's. Je kunt opzoeken of je al in eduGAIN geregistreerd staat (is het geval voor de meeste IdP's). Indien niet, kan degene met de rol 'SURFconextverantwoordelijke' aan SURFconext vragen de IdP te voegen aan eduGAIN. Dit kan hij/zij door in het SURFconext Dashboard (tabje "Mijn instelling", knop "Wijzigingsverzoek aanmaken", vinkje "Gepubliceerd in eduGAIN" aanvinken). Weet je niet wie binnen jouw instelling de rol 'SURFconextverantwoordelijke' heeft? Zoek dit desnoods op in dashboard.surfnet.nl

  Na het publiceren van je IdP in eduGAIN duurt het nog enige uren voor DigiCert dat verwerkt heeft.
- Tegelijkertijd kan de 'SURFconextverantwoordelijke' via het SURFconext Dashboard aangeven dat de instelling de DigiCert Service Provider wil gaan gebruiken. De bedoelde Service Provider heet in het Dashboard "DigiCert's TCS Portal - Digicert | Digicert"

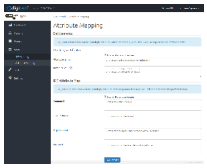
- Er is een manual beschikbaar. Voor *SURFconext klanten* is het laatste hoofdstukje 'How to Add an Organization Mapping (Participant SAML Admin)' belangrijk.

- **LET OP: ernstge bug GEEN NIEUWE SAML admin ROLLEN AANMAKEN zonder overleg met scs-ra@surfnet.nl**

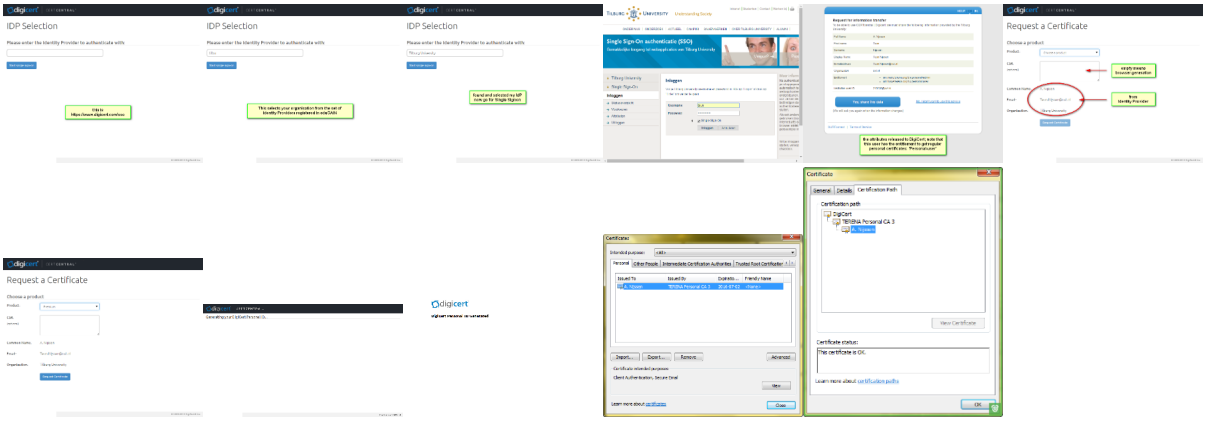
- Vervolgens vraagt iemand die al administrator is in de DigiCert portal om de aanvullende rol 'SAML admin' en hij voegt de mapping toe van de organisatie aan de IdP. Die mapping is technisch nauwkeurig uitgedrukt de waarde van het attribuut urn:mace:terena.org:attribute-def:schacHomeOrganization. Meestal is de waarde je hoofddomain, bijvoorbeeld uvt.nl Je vindt de inhoud als *organization*, in profile.surfconext.nl onder "My Profile"/"Mijn Profiel". Screenshotjes:



- SURFnet gebruikt op de DigiCert server voor al haar SURFconext klanten de attribute mapping die in het volgende screen shotje staat. Merk op dat daarin bij de entitlement zowel urn:mace:terena.org:tcs:personal-user als urn:mace:terena.org:tcs:escience-user genoemd zijn. Dit betekent in de DigiCert Portal dat slechts één van die twee entitlements voldoende is om de portal **www.digicert.com/sso** in te kunnen. Daar kunnen alle drie de types certificaten besteld worden. Dus met alleen de bevoegdheid urn:mace:terena.org:tcs:personal-user kan iemand een normaal 'Premium' persoonlijk certificaat en/of een eScience 'Grid Premium' persoonlijk certificaat en/of een 'Grid Robot Name' certificaat bestellen.



- Nadat je setup in orde is kan een gebruiker aanvragen doen voor Premium, of Grid Premium, of Grid Robot Name persoonlijke certificaten. Als je niet deelneemt aan de eScience Grid community wil je een Premium certificaat hebben voor bijvoorbeeld Client Authentication, Document Signing, Email Encryption of Email Signing. Screenshotjes:



voor de techneuten staat hieronder de inhoud van het resulterende certificaat

```
$ openssl x509 -noout -text -inform der -in nijssen.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0b:9d:27:e4:23:0c:14:00:75:5b:90:2d:4c:24:ed:22
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Personal CA 3
        Validity
            Not Before: Jul  2 00:00:00 2015 GMT
            Not After : Jul  2 12:00:00 2016 GMT
        Subject: C=NL, ST=Noord Brabant, L=Tilburg, O=Tilburg University, CN=A. Nijssen
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c7:01:91:87:b0:51:5a:6f:46:68:78:4b:cf:a5:
                    62:23:70:fc:dd:c3:53:5a:5c:34:12:dc:da:3f:0f:
                    fa:e3:2e:fc:c8:10:1b:83:7b:72:34:4e:ed:39:81:
                    b1:e7:39:56:a8:bd:bc:2c:6b:8d:0c:6b:54:d5:3f:
                    e0:bc:e3:e8:88:a6:f9:42:7c:f7:96:83:7c:16:36:
                    b2:22:8a:ea:d4:a0:e8:29:1a:be:4a:84:a2:19:9b:
                    be:ab:a5:05:6d:9e:de:20:d1:70:30:0d:60:18:d0:
                    63:2d:ed:cb:f8:55:80:51:57:bc:cf:b6:30:c7:ea:
                    cb:20:76:83:f8:c0:dc:1c:d2:39:65:77:91:35:75:
                    a8:e9:b1:c7:70:d0:bd:b1:6a:27:0f:4f:7d:9b:ba:
                    9b:ba:c9:f0:64:09:36:2b:8e:48:93:93:a9:b6:00:
                    af:b7:c5:aa:25:2c:6d:e5:dc:62:51:06:ae:eb:fe:
                    59:69:06:98:64:b1:3c:c0:c2:2b:ba:ed:13:83:68:
                    84:9e:37:cb:88:f3:32:75:63:47:81:ea:ba:1c:a2:
                    82:01:a8:b3:99:95:f5:ab:9d:d7:6f:bb:e9:ed:d6:
                    9a:10:9b:9d:42:30:65:46:9d:d5:19:55:49:05:fe:
                    31:01:0f:b8:cb:22:d1:05:78:3b:49:72:37:09:50:
                    0f:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA
            X509v3 Subject Key Identifier:
                0E:97:EE:E2:D1:CF:97:C1:0F:36:25:D6:48:C1:DC:5E:C0:2F:0F:AE
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Alternative Name:
                email:Teun.Nijssen@uvt.nl
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114412.4.1.2
                  CPS: https://www.digicert.com/CPS
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl3.digicert.com/TERENAPersonalCA3.crl
                Full Name:
```

```
                URI:http://crl4.digicert.com/TERENAPersonalCA3.crl
            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com
                CA Issuers - URI:http://cacerts.digicert.com/TERENAPersonalCA3.crt
    Signature Algorithm: sha256WithRSAEncryption
         0a:9d:60:fd:a3:9e:44:24:f2:47:d0:59:85:b9:50:6b:63:05:
         b2:3d:1b:99:e9:38:4c:dc:fe:36:98:cd:fb:75:41:41:e9:12:
         30:84:41:55:86:c6:51:e1:29:57:8e:71:e6:b2:a7:6f:36:32:
         23:ab:9c:63:c3:3a:88:27:48:fd:41:83:fc:27:55:ba:e1:a2:
         33:06:bc:4f:93:0c:7d:ea:c6:d5:be:a9:f8:66:14:b6:53:45:
         97:4e:e1:e6:15:6a:15:70:c4:12:34:4f:93:14:de:1e:0a:d1:
         8b:e4:8d:a2:82:3d:40:a4:84:af:7c:b5:3a:8e:4d:e8:6b:38:
         35:f4:4d:d0:c8:f6:97:4a:d2:11:c2:c3:fb:4b:d7:75:bf:84:
         39:14:4f:bb:33:aa:b9:42:72:3f:f1:ad:cb:65:ba:58:e5:1b:
         18:7f:62:c8:d9:2e:77:c4:59:0a:33:88:1a:c8:2b:1e:50:4a:
         45:0c:2f:7f:e4:d8:2d:fc:9c:8c:a5:35:7b:c8:4f:a2:0d:14:
         f8:8c:73:d5:58:26:2a:a6:f9:a1:24:3d:3b:24:b7:8e:01:a6:
         fa:7d:82:1b:16:60:3f:67:e4:b8:ed:c4:f5:53:80:e1:94:c1:
         e2:06:f0:ca:11:d0:80:17:3a:f3:bd:24:7a:db:67:d0:67:9d:
         f2:dd:b5:91
```