Persoonscertificaten aanvragen

Met persoonscertificaten bedoelen we certificaten die gebruikt worden om publieke sleutels te binden aan personen (dit in tegenstelling tot servercertificaten, die publieke sleutels binden aan servers).

Om een persoonscertificaat aan te vragen maak je gebruik van de portal https://cert-manager.com/customer/surfnet/idp/clientgeant.

Voordat er kan worden ingelogd op deze portal moet de SCHAC Home Organization zijn ingesteld, zodat Sectigo kan bepalen bij welke organisatie een gebruiker hoort. Of dit is ingesteld kan worden gecontroleerd binnen SCM, door naar Organizations <eigen organisatie> Edit (potlood rechts) te gaan en te kijken wat er onder *Academic code (SCHAC Home Organization)* staat. Als dit niet correct is kan dit worden ingesteld door een verzoek in te dienen via certificaten-beheer@surf.nl

De persoon waar het certificaat voor bedoeld is wordt bepaald door de volgende attributen die, na authenticatie via SURFconext, worden verkregen:

friendly name	SAML attribute name	voorbeeld	verplicht?
mail	urn:oid:0.9.2342.19200300.100.1.3	johndoe@example.edu	ja
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	jd@example.edu	alleen voor grid/robot certificates
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	urn:mace:terena.org:tcs:personal-user	ja (voor autorisatie)
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	example.edu	ja
cn	urn:oid:2.5.4.3	John Doe	alternatief voor CN
sn	urn:oid:2.5.4.4	Doe	alternatief voor CN
givenName	urn:oid:2.5.4.42	John	alternatief voor CN
displayName	urn:oid:2.16.840.1.113730.3.1.241	Johnny Doe	ja, voor CN

Bij het ontbreken van een displayName wordt het CN veld geconstrueerd uit givenName+sn of cn.

Voor de verschillende soorten sleutels, zie Soorten Certificaten.

Sleutelmateriaal

Sleutelmateriaal voor certificaten bestaat uit twee delen: een publiek deel en een privaat deel. Het publieke deel wordt opgenomen als onderdeel van het certificaat bij uitgifte door de CA. Het private deel moet zorgvuldig worden opgeslagen door de persoon waarvoor het certificaat bedoeld is. Het private deel wordt immers gebruikt door de persoon om zich te authenticeren, of om versleutelde berichten te ontcijferen.

Voorheen werd sleutelmateriaal aangemaakt door de browser via een speciaal daarvoor bedoeld HTML element (<keygen>), zodat het private deel veilig in de client (browser) kon worden opgeslagen en het publieke deel naar de CA kon worden gestuurd. Moderne browsers ondersteunen dit echter niet langer, waardoor Sectigo de mogelijkheid biedt het sleutelmateriaal op de server te genereren. Zowel het private deel als het publieke deel (ingebed in het certificaat) kunnen vervolgens in een zogeheten PKCS#12 bestand worden gedownload. het private deel wordt in dat geval beschermd door een wachtwoord dat de gebruiker zelf kiest. Ook kan de gebruiker kiezen tussen RSA en ECC sleutels.

Gebruikers die niet willen dat het sleutelmateriaal op de server wordt gegenereerd, hebben twee alternatieven:

1. genereer het sleutelmateriaal zelf met daarvoor geschikte tools (bij voorbeeld openssl) en upload alleen het publieke deel in de vorm van een PKCS#10 Certificate Signing Request naar de server.
2. gebruik een alternatieve portal, die gebruik maakt van de JavaScript WebCrypto API. Gebruik van deze portal is momenteel op basis van opt-in (niet voor IGTF/Grid certificaten). Neem contact op met certificaten-beheer@surf.nl