FAQ

Wat kost de dienst SURFcertificaten?

SURFcertificaten kost in 2020 136 euro per maand, exclusief btw. Dit is een flat-fee tarief; u kunt zoveel certificaten aanvragen en van ieder type (m.u.v. document-signing) zonder meerprijs.

Welk type certificaten levert SURFnet via SURFcertificaten?

De dienst SURFcertificaten omvat de volgende type certificaten:

- Server
- Persoonlijke, ook wel client- / e-mailcertificaten
- Code-signing
- Document-signing (vereist goedgekeurd hardware token)
- eScience (IGTF)

In welke situaties heb ik een EV-certificate nodig?

Maak met mate gebruik van Extended Validation certificates. Gebruik deze wel voor uw belangrijke publiekswebsites, maar niet voor server-server verbindingen die een mens nooit ziet en evenmin voor testen. Kies een eigen beleid dat recht doet aan de gebruiksvoorwaarden.

Hoe kan ik nieuwe gebruikers machtigen om certificaten aan te vragen?

Het toevoegen/ verwijderen van gemachtigde gebruikers om certificaten aan te vragen wordt ingesteld in het Sectigo certificate management portaal.

- Een RAO (Registration Authority Officer) kan extra RAO's aanmaken. De rechten worden toegekend door de MRAO (Master Registration Authority Officer) van SURFcertificaten.

Stuur na het aanmaken van de nieuwe RAO een verzoek naar scs-ra@surfnet.nl om de juiste rechten toe te kennen.

- Alle RAO accounts kunnen certificates aanvragen, en de certificate requests goedkeuren of afwijzen.

Geen idee wie er voor jouw instelling de RAO is? Vraag het ons even via scs-ra@surfnet.nl. We helpen je graag verder.

Mag ik een functioneel account opvoeren als RAO account?

NEE. Op deze manier is immers niet te achterhalen welke gebruiker welke certificaten aanvraagt of goedkeurt. De RAO heeft een persoonlijk email-account bij de instelling (bijv. bart.bosma@surfnet.nl).

Is het mogelijk om een wildcard certificaat aan te vragen voor een hoofddomein, bijv. surfnet.nl?

Dat kan technisch wel, maar dit is niet verstandig en raden wij daarom ten zeerste af.

Bedenk bij het installeren van een wildcard certificaat op een server wat er gaat gebeuren als de private key op een van die servers gecompromitteerd raakt. Hoe meer servers, hoe groter de ellende, ervan uitgaande dat je nog precies weet op welke servers dat certificaat allemaal staat.

De overweging is dat als bijvoorbeeld een faculteit zo'n certificaat zou hebben, dat draait op een gehackte machine, dat ook de machines van een andere faculteit gevaar lopen, zonder dat die zich daarvan bewust zijn. Het is dan verstandiger om *.subdomain.instelling.nl te gebruiken.

Het is overigens een fluitje van een cent om elke server een eigen certificaat te geven. Alleen in geval van certificaten op clusters e.d. kunnen wildcard certificaten een belangrijke toepassing zijn.

Wat gebeurt er met onze oude DigiCert-certificaten na afloop van het contract op 30 april 2020?

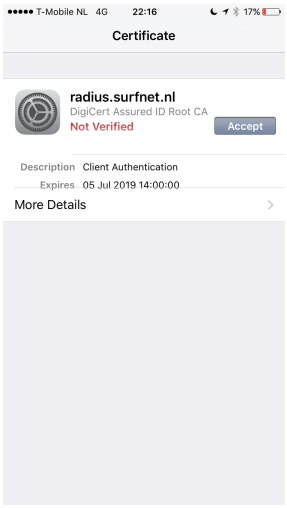
Deze blijven ook na 30-4-2020 geldig tot het einde van de geldigheidsduur die het certificaat bij uitgifte heeft meegekregen (1,2, of 3 jaar).

Waarom krijgen mijn gebruikers een certificaat-popup "Not Verified" als ze met eduroam verbinden op hun iPhone?

Dit issue heeft te maken met de manier waarop eduroam (of meer specifiek, 802.1X) werkt: typisch wordt TLS gebruikt voor server authenticatie op het moment dat de supplicant contact opneemt met een access point voor authenticatie. Authenticatie vindt echter plaats via RADIUS (bv EAP-TTLS) en om user credentials niet aan het access point bloot te geven wordt een TLS tunnel opgebouwd naar de RADIUS server. Omdat de supplicant a priori niet weet welke RADIUS server dit is (in het geval van eduroam loopt de tunnel door meerdere tussenliggende RADIUS servers), kan de supplicant niet de subject DN van het certificaat vergelijken met de hostnaam van de RADIUS server (zoals een webbrowser de hostnaam in de URL vergelijk met die in het certificaat).

Dat betekent dat de gebruiker een waarschuwing krijgt, zodat kan worden gecontroleerd of de tunnel op de juiste RADIUS server termineert. Er is dus niets mis met het certificaat, de melding betekent alleen dat niet automatisch kan worden geverifieerd dat dit de server is waar je verbinding mee wilt leggen.

Overigens gebeurt dit alleen de eerste keer dat je met het netwerk verbindt, daarna wordt het certificaat gecachet en als vertrouwd beschouwd (button *Accept*). Zie screenshot. “Not verified” betekent dus “het certificaat klopt maar ik weet niet of dit certificaat behoort bij de gewenste server”.



Als je de melding wilt voorkomen zou je het certificaat, of op zijn minst de naam van de RADIUS server, vooraf bekend moeten maken aan het iOS device. Dat kan bijvoorbeeld via een iOS profile gemaakt met Apple Configurator 2. Zie https://support.apple.com/en-gb/HT207866

Waarom krijgen mijn Apple gebruikers een certificaat-popup "Not Trusted" ("Niet Vertrouwd") als ze met eduroam verbinden?

Gebruikers kunnen ook een popup krijgen met de melding “Not trusted”. Dit betekent “ik kan het certificaat niet valideren”, typisch omdat een CA certificaat ontbreekt. In dat geval is de RADIUS server niet juist geconfigureerd. Voor Digicert certificaten dient het TERENA SSL CA 3 intermediate certificaat worden toegevoegd.

Neem contact op met uw lokale eduroam beheerder om dit probleem op te lossen (Radiator hint: EAPTLS_CertificateChainFile)

Hoe gaat Sectigo om met een DNS CAA Resource Record Check?

Zie daarvoor de Sectigo support site.

Om een CAA record aan te maken kun je de Sectigo CAA-record generator Tool gebruiken. Zones die worden gehost via www.surfdomeinen.nl kunnen van CAA records worden voorzien door gedelegeerden met de rol *DNS-Beheerder*. Zie daarvoor ook de handleiding van SURFdomeinen.