FAQ

Wat kost de dienst SURFcertificaten?

Een link naar actuele prijzen vind je op de productpagina: https://www.surf.nl/surfcertificaten-versleutelde-verbindingen-met-je-webservers

Waar vind ik de documentatie?

Een snelstart-handleiding is te vinden op: https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA03l000000vFnd

Volledige beheerdershandleidingen (inclusief API-documenten) zijn te vinden op: https://support.sectigo.com/Com_KnowledgeProductPage?c=Admin_Guides&k=&lang=

Is er op dit moment een storing?

De status van de dienst is te raadplegen op https://sectigo.status.io/pages/5938a0dbef3e6af26b001921. Bij grote storingen zullen we altijd naar het scs-ra mailadres wat je bij het in gebruik nemen van de dienst hebt aangemaakt communiceren.

In welke situaties heb ik een EV-certificaat nodig?

Maak met mate gebruik van Extended Validation certificaten. Deze certificaten vereisen extra validatie, terwijl deze extra validatie tegenwoordig niet meer direct zichtbaar is in browsers. Kies een eigen beleid dat recht doet aan de gebruiksvoorwaarden. Meer details over het aanvraagproces zijn te vinden op EV servercertificaten.

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

Dat kan technisch wel, maar we raden het 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.

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.

Kan ik meerdere SAN's toevoegen, of deze wijzigen bij een *renewal*

Ja. Je hoeft deze ook niet per sé in het CSR op te nemen, dit kan ook in de SCM-interface. Let er op dat domeinen gescheiden worden door een comma.

Hoe ga ik om met niet-ASCII-tekens voor (IGTF) certificaten?

IGTF-certificaten mogen geen niet-ASCII-tekens bevatten. Er zijn verschillende manieren om dit te regelen:

- Als je organisatienaam niet-ASCII-tekens bevat, voer dan een ASCII-versie in in het vak "Secundaire organisatienaam" onder Instellingen. Bijvoorbeeld GÉANT Vereniging wordt GEANT Vereniging.
- Probeer de velden die je invult voor het certificaat te beperken - het is alleen nodig om Plaats en Land in te vullen.
- Sectigo kan de velden na validatie aanpassen zodat ze ook ASCII-tekens bevatten. Neem hiervoor contact op met de helpdesk.
- Als je er de voorkeur aan geeft om niet-ASCII-tekens binnen uw normale certificaten te houden, kan je een tweede organisatie maken met dezelfde gegevens, maar met niet-ASCII-tekens ingevuld. We raden je aan om de helpdesk te waarschuwen dat dit je bedoeling is.

Hoe kan ik een .csr bestand maken?

Er is hier een eenvoudig hulpmiddel om OpenSSL .csr-bestanden te maken: https://www.digicert.com/easy-csr/openssl.htm.

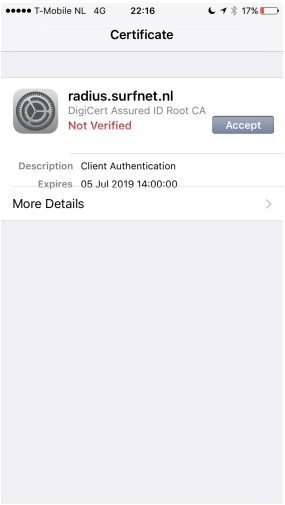
Sectigo biedt hier een handleiding voor het maken van .csr-bestanden: https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFIo.

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 en deze wiki-pagina.

Hoe kan ik java code signeren met een hardware token?

Voor het signeren van JAVA-code kun je gebruik maken van de handleiding van Oracle. Deze is wel achter een beveiligde omgeving van Oracle zelf:

https://support.oracle.com/knowledge/Oracle%20E-Business%20Suite/2806640_1.html

Waarom blijft mijn aanvraag op 'applied' of 'pending' hangen?

Check voor je aanvraag de volgende zaken:

1. CAA records van alle FQDN's & domeinen in de certificaataanvraag. Let hier ook op de tag "issuewild" (van belang bij wildcard certificaten).

2. Umlauten, diakritische tekens enz. in de org-naam of provincie/staat enz.
dat zorgde voor een handmatige controle van de eerste aanvraag die deze tekens bevatte door Sectigo en kan dus langer duren

3. org namen die precies 64 *bytes* zijn en let op dat enkele UTF-8 karakters
kunnen tellen als 2 bytes

4. geblokkeerde woorden in de aangevraagde domeinen zoals "test", "demo" enz.,

5. sommige zeer speciale coderingen van ECC-sleutels veroorzaken vastgelopen certificeringsaanvragen

6. redenen gegeven door de Sectigo Order Checker
https://secure.trust-provider.com/products/ORDERSTATUSCHECKER

2 en 4 zullen altijd een handmatige check by Sectigo vereisen, waardoor het langer duurt (als het al vanzelf gaat). Daarnaast heeft Sectigo soms onverklaarbare vertraging. Dien in dat geval een ticket in op https://www.sectigo.com/support-ticket met het ordernummer. Selecteer Case type: Technical Support en case reason: Sectigo Certificate Manager (SCM) om het snelst geholpen te worden.

Als de certificaten na 24 uur nog steeds niet zijn goedgekeurd zonder het vermoeden dat het aan een van het bovenstaande ligt we je vragen om de CSR naar ons te mailen via certificaten-beheer@surf.nl, dan kijken we met je mee.

Waarom zijn er nu ook 'authenticatie' SURFcertificaten?

Het CA/Browser forum wat de certificaatstandaarden bepaald heeft in 2023 een assurance baseline en specifieke technische profielen voor S/MIME certificaten geïntroduceerd die van invloed heeft op het soort certificaten wat we kunnen aanbieden. Door de vertrouwens- en betrouwbaarheidsniveaus die in deze S/MIME-basisvereisten zijn gedefinieerd maken de technische profielen die voor S/MIME BR worden beoogd het onmogelijk om één enkele CA van afgifte en één enkele openbaar vertrouwde root-CA te blijven gebruiken voor zowel persoonlijke e-mailcertificaten voor ondertekening als voor clientauthenticatie.

We zijn tot de conclusie gekomen dat het scheiden van de e-mail S/MIME-*use-cases* en de clientauthenticatie-*use-cases* de beste manier is om verder te gaan. Clientauthenticatie zal worden verzorgd door een onafhankelijk, gemeenschapspecifiek vertrouwensmodel (d.w.z. een privé CA), en we zullen de publiek vertrouwde S/MIME CA dienst beschikbaar houden voor e-mail ondertekening en encryptie gebruikssituaties.

Zowel een publieke-trust dienst als een private-CA dienst zullen parallel worden uitgevoerd en beide zullen beschikbaar zijn voor de gehele TCS gemeenschap op basis van de huidige assurance praktijken. **De private-CA certificaten zijn een vervanging van de IGTF authenticatiecertificaten (voorheen (GÉANT) IGTF-MICS (Robot) Personal/Email).**

Wat is er gebeurd met de lijst van profielen in het 'clientgeant' (SAML) portaal?

Het '/clientgeant' SAML portaal zal zo snel mogelijk de twee nieuwe profielen toevoegen naast de huidige. Dus "GEANT Personal Authentication" (private trust individuele authenticatie) en "GEANT Personal Automated Authentication" (private trust agent authenticatie voor ‘robot’-toepassingen) zullen aan de lijst worden toegevoegd.

Na 28 augustus worden de oude "GEANT IGTF MICS Personal" en "GEANT IGTF MICS Personal Robot" verwijderd van het SAML-portaal. Tegelijkertijd zal het "GEANT Personal" profiel (dat hernoemd zal worden naar "e-mail ondertekening en encryptie") een public-trust S/MIME only e-mail ondertekening en encryptie profiel worden. Dit openbare S/MIME-profiel zal het door de organisatie gevalideerde profiel gebruiken om de voor- en achternaam van de aanvrager in te voegen naast de naam van de organisatie.

Ik heb (zomer 2023) partijen binnen mijn instelling die clientauthenticatie gebruiken voor diensten (websitetoegang, IdP-login, eduroam, ...). Moeten zij actie ondernemen?

Ja, systemen die TCS Personal en eScience Personal certificaten gebruiken moeten actie ondernemen voor 28 augustus 2023. Er zijn een paar scenario's:

- de dienst maakt gebruik van GEANT eScience Personal (unieke) cliëntcertificaten: installeer de nieuwe "Research and Education Trust" certificaten, en - afhankelijk van de cliënttoepassing - ook de "GEANT TCS Authentication RSA/ECC CA 4B". Deze kunnen gevonden worden in de TCS Repository. Alle relevante certificaten worden ook verspreid door de IGTF in distributieversies 1.122 en hoger (ECC-varianten in versie 1.123). De onderwerpnaamgeving van de eindgebruikers blijft hetzelfde. Na 28 augustus kunnen

aanvragers geen eScience Personal-certificaten meer aanvragen bij de gezamenlijke-trust eScience Personal (ECC) CA 4. Deze optie wordt verwijderd van het clientgeant-portaal. Reeds uitgegeven certificaten blijven geldig gedurende de gehele aangegeven periode.
- de dienst gebruikt GEANT Personal (alleen CN) cliëntcertificaten: bekijk het geval zorgvuldig. Als de authenticatie afhankelijk is van de onderwerpnaam in het certificaat, moet je er rekening mee houden dat deze naam niet gegarandeerd uniek is. Er kunnen meerdere gebruikers zijn die uiteindelijk dezelfde onderwerpnaam krijgen. Je wordt aangeraden om over te stappen naar de nieuwe "Research and Education Trust" en de "GEANT TCS Authentication RSA/ECC CA 4B".
  Als je besluit om bij de huidige GEANT Personal CA 4 S/MIME e-mailcertificaten te blijven, let er dan op dat de opmaak van de onderwerpnaam zal veranderen: deze bevat mogelijk geen commonName meer, zal givenName en SN attributen bevatten, en kan andere RDN componenten bevatten die momenteel niet aanwezig zijn in de opmaak van de naam.
- de dienst maakt gebruik van GEANT eScience Personal Robots voor rolgebaseerde authenticatie (bijv. monitoring agents, data movement agents, etc.): installeer de nieuwe "Research and Education Trust" certificaten, en - afhankelijk van de client applicatie - ook de "GEANT TCS Authentication RSA/ECC CA 4B". Via het SCM invite proces vraag je een "GEANT Organisation Automated Authentication" certificaat aan voor deze gebruikers.
- de dienst maakt gebruik van GEANT eScience Personal Robots voor het verzenden van e-mails (herondertekening van maillijstservers, geautomatiseerde verzending door rollen zoals beveiligingsteams die gebruikersberichten verzenden, enz. Dit betekent dat je de GEANT Personal CA 4 kan blijven gebruiken, maar in SCM "GEANT Organisation e-mail signing" moet aanvragen. Het profiel "GEANT IGTF Robot Email" is dus opgesplitst naar doel: er zijn twee nieuwe profielen, één private trust voor authenticatie, één public trust voor door de organisatie gevalideerde S/MIME!

Moet mijn organisatie opnieuw worden gevalideerd om S/MIME-certificaten uit te geven na 28 augustus 2023?

Ja, door kleine verschillen in devereisten is de set 'authentieke informatiebronnen' die Sectigo moet gebruiken voor organisatievalidatie anders. Terwijl voor SSL-validatie een onafhankelijke informatiebron mag worden gebruikt, zijn voor S/MIME alleen bronnen van overheidsinstanties en gegevensreferenties van de Legal Entity Identifier (LEI) toegestaan. Dit betekent dat Sectigo opnieuw moet valideren. Dit gebeurt niet automatisch - abonnees moeten dit via SCM in gang zetten. Voor alle organisaties die meer dan 10 actieve persoonscertificaten had is dit door SURF op de achtergrond in gang gezet. Voor de overige organisaties wordt deze validatie automatisch gedaan bij de eerstvolgende her-validatie, meestal aan het einde van het jaar. Neem contact met ons op als de certificaten in de tussentijd al nodig zijn.

Hoe gaan SURF, GÉANT en Sectigo om met de AVG?

Sectigo heeft een gedetailleerde Privacyverklaring beschikbaar voor alle gebruikers. Als onderdeel van het inkoopproces zijn de gegevensbeschermings- en beveiligingsmaatregelen bij Sectigo geëvalueerd volgens het standaardproces van GÉANT voor de inkoop van diensten. Het GDPR-team van GÉANT heeft een document opgesteld met hun algemene beoordeling van de privacypositie voor Sectigo.

Mijn vraag staat hier niet bij, wat nu?

Mail ons op certificaten-beheer@surf.nl, dan heb je binnen twee werkdagen antwoord. Zie ook Contact en Ondersteuning.