Workshops en Nieuwsberichtenarchief

maart 2024

Beste gebruikers van SURFcertificatem

Hieronder een update over ontwikkelingen rondom de dienst, die sindskort volledig ISO27001 gecertificeerd!

Initiatief rondom 2FA en accountrechten

Zoals jullie gemerkt hebben zijn we flink aan het pushen op 2FA en het checken van de rechten van jullie admin-accounts. Je ontvangt hier nu maandelijks (later 3-maandelijks) een automatisch gegenereerd rapport over, en vanaf 1 juni gaan we accounts zonder 2FA uitschakelen (API-accounts uitgezonderd). Om vragen zo veel mogelijk op te vangen hebben we o.a. de documentatie over Inloggen met SURFconext, het omzetten van andere accounts en 2FA via SURFconext of met een persoonscertificaat herzien. We wijzen jullie ook graag op de mogelijkheid om ACL's in te stellen als dat past bij je risico-inschatting.

Enrollment forms en ACME

Een veelgestelde vraag is hoe je als instelling het proces rondom uit uitgeven van certificaten aan eindgebruikers of leveranciers makkelijker kan maken, zeker als je niet iedereen een account in SCM wil geven. Twee opties kunnen daarbij helpen: Enrollment Forms:aanvraagformulieren voor eindgebruikers en ACME: geautomatiseerde uitgifte van certificaten voor (web)servers. Van beide zijn de documentatie herzien. We hebben inmiddels veel ervaring opgedaan met verschillende implementatie. Heb je succesverhalen over jullie ACME implementatietraject? We horen het graag, dan maken we er een praktijkvoorbeeld van.

Contact via scs-ra@instelling.nl

De afgelopen jaren hebben we altijd primair gecommuniceerd via het scs-ra adres van de instellingen. Helaas merken we dat het bijhouden van dat adres nogal eens wordt vergeten, waardoor we bij belangrijke zaken vaak tóch direct een aantal beheerders mailen. Vanaf heden gaan we dat standaard doen: we mailen voor dit soort mail-to-all's alle beheerders die rechten hebben om andere beheerders te wijzigen, en zien dat als de 'belangrijke' beheerders.

Meedenken over de toekomst

Vanuit GÉANT worden diverse sessies georganiseerd over de toekomst van de certificaatdienstverlening door NREN's (lees: SURFen) in Europa. Wil je graag meedenken over de toekomst van de dienst? Ook dan horen we graag van je. In onze antwoorden op supportvragen is het antwoord nog wel eens "Dat ligt aan Sectigo en daar kunnen we weinig aan veranderen": dit is het moment om iets met al díe vragen te doen

Introductietraining SURFcertificaten

We hebben onlangs een introductietraining over de dienst aangekondigd. De online versie van die training gaan we binnenkort inplannen, maar eerst geven we deze training over een paar weken aan interne collega's. Op basis van de ervaringen passen we de training aan om deze geschikt te maken voor de online opstelling. Als je van plan was naar SURF te komen om de live versie bij te wonen en je hebt je aangemeld, dan ben je nog steeds van harte welkom, maar misschien wacht je liever op de online versie i.v.m. de reistijd.

Vragen over deze mail kun je sturen naar: certificaten-beheer@surf.nl. Heb je oude berichten gemist? Zie ook onze wiki: Workshops en Nieuwsberichtenarchief

Met vriendelijke groet / Kind regards,

SURFcertificaten team

10 januari 2024

Beste SURFcertificaten-gebruiker,

Een groot aantal admin-gebruikers van de SURFcertificaten-portal (Sectigo Certificate Manager) maakt nog geen gebruik van SURFconext of 2FA bij het inloggen op deze portal. Dat levert niet alleen een aanzienlijk beveiligingsrisico op voor je eigen instelling, maar is ook niet in lijn met de rest van de SURF-diensten. Het is daarmee ook een aandachtspunt bij onze recente ISO 27001 certificeering.

We vragen je daarom om vóór 1 maart per admin-account:

Inloggen via SURFconext te activeren. Lees hier de handleiding: https://wiki.surfnet.nl/display/SCERTS/Inloggen+via+SURFconext óf
2FA in te stellen met een persoonscertificaat als tweede factor - als je instelling geen gebruik maakt van SURFconext. Lees hier de handleiding: https://wiki.surfnet.nl/display/SCERTS/2FA+met+persoonscertificaat

Niet voor 1 maart geactiveerd: herinnering en uiteindelijk deactivatie van het account

Vanaf 1 februari ontvang je maandelijks geautomatiseerde rapportages over beveiligings- en rechtenkwesties van de SCM-accounts van je organisatie.

Als 2FA niet voor 1 maart is geactiveerd, ontvang je tot 1 juni herinneringsmails, uitgezonderd de API-accounts.

Als er na 1 juni geen actie is ondernomen, gaan we er van uit dat het account niet meer in gebruik is en wordt het op non-actief gezet. Dit betekent dat er niet meer mee ingelogd kan worden.

Mocht je één account als 'break the glass' optie buiten SURFconext om willen laten inloggen kan dat, maar voeg dan wel 2FA met een persoonscertificaat toe. Een account kan ook zowel via SURFconext als met wachtwoord inloggen (zie SURFconext handleiding).

We realiseren ons dat het een ingrijpende maatregel is. Maar gezien de mogelijke impact, is het wel een noodzakelijke. Daarnaast gaan er van uit dat het zo ver niet komt en dat we constructief kunnen samenwerken om onze beveiliging van de portal te verbeteren. Als je vragen, zorgen of iets anders hebt, stuur dan een e-mail naar: certificaten-beheer@surf.nl.

Niet mogelijk om 2FA te gebruiken? Neem dan contact op!

Als er omstandigheden zijn waardoor je instelling geen 2FA kan gebruiken, laat het ons te dan weten via certificaten-beheer@surf.nl. Dan zoeken we samen naar een oplossing. Bij voorbaat dank!

Dank je wel voor je tijd en aandacht, en laten we samen zorgen voor een veiligere omgeving voor ons allemaal

Met vriendelijke groet / Kind regards,

SURFcertificaten team

17 oktober 2023

Beste gebruiker van SURFcertificaten,

De resultaten van de ACME-survey zijn nu binnen, dank voor het invullen van de vragenlijst!

We organiseren twee onlinebijeenkomsten van gebruikersgroepen, een in november en de andere in januari. Sluit je vooral aan om handvatten te krijgen bij het implementeren van ACME en dit is een goede kans om je vragen te stellen en misschien instellingen te vinden waarmee je kunt samenwerken.

De sessies dien je zelf in je agenda te zetten, en vooraf inschrijven of aanmelden is niet nodig. De sessies vinden plaats op de volgende data:

30 november, 13:00 – 15:00 en 15 januari, 14:00 – 16:00

De Teams-links heb je in een email naar het scs-ra-adres van je instelling gekregen.

Met vriendelijke groet / Kind regards,

SURFcertificaten team

11 augustus 2023

Beste gebruiker van SURFcertificaten,

Hieronder een update over ontwikkelingen rondom de dienst, waaronder één met een hoge urgentie, over het gebruik van persoonscertificaten voor authenticatie.

Nieuwe richtlijnen en *private trust hierarchy* voor persoonscertificaten

Als gevolg van nieuwe standaarden bepaald door het CA/Browser Forum zullen we eind deze maand (28 augustus) nieuwe authenticatiecertificaten introduceren. Voor 'normale' persoonscertificaten (ook bekend als S/MIME certificaten) voor bijvoorbeeld email-ondertekening en encryptie verandert er weinig. Sectigo zal voor sommige organisaties wat extra organisatievalidatiestappen moeten uitvoeren, daar krijg je dan vanzelf bericht over. Wat wel belangrijk is om te weten is dat de *common name* van dit certificaat niet langer als uniek kan worden beschouwd en het certificaat dus ongeschikt is voor authenticatiedoeleinden.

Aan de IGTF authenticatiecertificaten (voorheen (GÉANT) IGTF-MICS (Robot) Personal/Email) verandert meer. Dit zijn vanaf de wijzigingen de enige certificaten die echt geschikt zijn voor authenticatie, en worden dan uitgegeven vanuit een *private trust hierarchy*. **Elk systeem wat dit type certificaten gebruikt voor authenticatie moet een nieuwe *trust anchor* toevoegen.** Om systeembeheerders hier extra tijd voor te geven hebben we alle gebruikers waarvan het authenticatiecertificaat binnen 99 dagen verloopt gevraagd om deze nu te vernieuwen, zodat de meeste systemen pas enkele weken na de wijziging met de nieuwe certificaten te maken krijgen.

Beheerders van systemen die certificaten voor authenticatie gebruiken moeten dus het nieuwe trust anchor toevoegen. Mocht je twijfelen of dit voor een specifiek systeem geldt, kijk dan even hier op de wiki voor de verschillende opties. De nieuwe trust anchors kan je vinden op https://wiki.geant.org/display/TCSNT/TCS+Trust+Anchors+and+Intermediates. Je kan ons bereiken op certificaten-beheer@surf.nl bij vragen. Ook hebben we hebben de FAQ uitgebreid met vragen die je zou kunnen hebben over de nieuwe situatie. De nieuwe certificaten zijn als volgt:

NEW PUBLIC TRUST

GEANT Personal email signing and encryption (ook in de /clientgeant portal)
GEANT Organisation email signing (NIET in de /clientgeant portal)

NEW PRIVATE TRUST

GEANT Personal Authentication (ook in /clientgeant)
GEANT Personal Automated Authentication (ook in /clientgeant)
GEANT Organisation Automated Authentication (NIET in /clientgeant)

Delegatie van *enrollment forms*

Een oplettende gebruiker (dankjewel!) wees ons er op dat veel organisaties hun *self-enrolment forms* (https://cert-manager.com/customer/surfnet?private#enrollment_forms) niet aan de eigen organisatie hadden gedelegeerd, waardoor de formulieren voor andere organisaties te zien en aan te passen waren. Wij hebben dit nu voor iedereen aangepast, maar let er dus op dat dit nog apart dient te gebeuren na het aanmaken. We werken op dit moment aan nieuwe documentatie voor enrollment forms in het algemeen, en code-signing specifiek.

Aankomende rapportages over admin-accounts

In het kader van de ISO-27001 certificering van SURFcertificaten zijn we verbeteringen aan het doorvoeren in het accountbeheer van SCM. Hoewel dit voor RAO-accounts een verantwoordelijkheid voor de instelling zelf is, zijn we voornemens om binnenkort elke instelling geautomatiseerd te laten weten welke verbeteringen er mogelijk zijn. Zo raden we aan om alleen nog IdP-accounts (via SURFconext) te gebruiken, 2FA in te schakelen, en zullen we bijvoorbeeld signaleren als er binnen je instelling slechts één persoon is die rechten toe kan kennen aan anderen. Hierover, en over andere verbeteringen aan de beveiliging van SCM, ontvangen jullie later een uitgebreidere update. Je kan alvast kijken naar de lijst van accounts en bijbehorende rechten om te controleren of het nog actueel en kloppend is. Schakel ook alvast 2FA aan en ga in gesprek met je SURFconext beheerder om inloggen via SURFconext aan te zetten. Wat daar verder voor nodig is lees je hier.

ACME

We zijn ook voornemens om na de zomer een bijeenkomst te organiseren voor SURFcertificaten-gebruikers. Specifiek gericht op ACME, maar ook algemener bedoeld om ervaringen uit te wisselen en informeel vragen te kunnen stellen.

We hopen je hiermee nu weer op de hoogte te hebben gebracht. Als je nog vragen hebt, neem dan gerust contact op met certificaten-beheer@surf.nl

Met vriendelijke groet / Kind regards,

SURFcertificaten team

25 april 2023

Beste gebruiker van SURFcertificaten,

We willen je graag op de hoogte brengen van enkele ontwikkelingen met betrekking tot de dienst.

Aankomende wijzigingen voor code signing certificaten: Sectigo heeft wijzigingen aangekondigd in de procedures rondom code signing certificaten. Deze wijzigingen gaan in op 8 mei, met als belangrijkste wijziging dat deze alleen nog op een door Sectigo geconfigureerde USB hardware security module (een Safenet 5110, in de meeste gevallen) worden uitgereikt. Daarnaast is het mogelijk om zelf een YubiKey FIPS aan te schaffen en te gebruiken. Meer informatie hierover vind je op hun website.

Automatisering en geldigheid van 90 dagen: Al sinds 2015 is binnen het CA/Browser Forum de trend dat de maximale toegestane geldigheidsduur van certificaten steeds korter wordt. Voor de meeste toepassingen is dat inmiddels 1 jaar. Het is niet de vraag óf, maar wanneer we gaan bewegen naar certificaten met een nog kortere geldigheid, zoals bijvoorbeeld al jaren het geval is bij Let's Encrypt en ZeroSSL met een geldigheid van 90 dagen. Daarom willen we nogmaals het belang van automatisering, bij voorkeur door middel van ACME, benadrukken. ACME is hét protocol wat gebruikt wordt door o.a. Let's Encrypt en ZeroSSL. Wat men vaak (nog) niet weet is dat SURFcertifcaten ook ACME aanbiedt en dat er slechts een kleine aanpassing nodig is om certficaten aan te vragen bij SURFcertificaten in plaats van bij de eerdergenoemde partijen, die dan bovendien Organisation Validated zijn in plaats van alleen Domain Validated. In de SCM administrator guide staan handleidingen voor veel verschillende soorten systemen. Als je hulp of advies nodig hebt, kun je altijd contact opnemen met certificaten-beheer@surf.nl. Vanuit GÉANT - Trusted Certificate Service (TCS) volgen wij uiteraard de ontwikkelingen bij het CA/Browser Forum op de voet.

Problemen met Sectigo support: Onlangs hebben sommigen van ons problemen ervaren met de support van Sectigo, zoals trage of onkundige reacties. Dit is via GÉANT aangekaart, en er zijn verbeteringen beloofd waarvan we voorzichtig al de eerste tekenen terugzien. Wat we zelf nog kunnen doen is bij het registreren van een ticket altijd als *case reason* 'Sectigo Certificate Manager' te kiezen, zodat het ticket in de juiste queue komt.

Duidelijkere richtlijnen voor persoonlijke S/MIME certificaten: Er komen duidelijkere richtlijnen vanuit het CA/Browser Forum voor persoonlijke S/MIME certificaten, voornamelijk over de verschillen tussen persoonscertificaten en certificaten gebruikt voor een specifiek mailadres. Voor een uitgebreide toelichting verwijzen we graag door naar de presentatie van David Groep van het Nikhef. Hier zullen we als SURF in te toekomst zeker nog meer mee aan de slag gaan. S/MIME wordt nu voorzichtig steeds meer gebruikt, en we zien dat er veel vragen over zijn.

Meer verschillende rechten en deze zelf kunnen toekennen in SCM: Sinds de update van afgelopen weekend kunnen RAO's, oftewel jullie, zelf nieuwe rechten toekennen aan mede-beheerders als je die rechten zelf al hebt. Eerder moest dit via ons. Aangezien de meeste RAO accounts ook al zelf nieuwe beheerders kunnen toevoegen, zorgt dit er voor dat er geen MRAO meer nodig is om bijvoorbeeld een vervanger of back-up beheerder toe te voegen.

We hopen je hiermee nu weer op de hoogte te hebben gebracht. Als je nog vragen hebt, neem dan gerust contact op met certificaten-beheer@surf.nl

Met vriendelijke groet / Kind regards,

SURFcertificaten team

Beschikbare presentaties

Workshop - opname 3 april 2020 (Sectigo Certificate Manager, API, SAML/SSO en ACME)

Workshop - opname 9 april 2020 (Sectigo Certificate Manager, API, SAML/SSO en ACME)

Workshop - opname 6 mei 2020 (Client Certificate Portal - in English)

Sectigo - Introduction (update 9 april)

Sectigo - Authentication & Automation v1.0.5