SUNET

SUNET TCS - hösten 2021

Agenda

- Problem och utmaningar
  - tidigare
  - pågående
  - kommande
- Praktiska råd
- Framtiden

SUNET

Tidigare: databasmigreringen

Databasmigrering i juni

- Måste göra DCV igen för alla domäner
  - Om man missar så utfärdas inte certifikaten
- Kan inte revokera äldre certifikat inne i SCM
  - Det finns metoder att använda vid säkerhetsincident
- ACME-problem

SUNET

Tidigare

Prestandaproblem i SCM vid vissa tillfällen

- Se https://sectigo.status.io/

SHA384-signaturer

- Finns rapporter om äldre system som inte klarar detta
- Vi jobbar på att få möjlighet att utfärda certifikat med SHA256 via SCM

SUNET

Pågående: åäö-fördröjning

- Ändring 25/9 där Sectigo införde extra kontroller av certifikat som har namn som inte är 100% ASCII, på grund av tidigare felutfärdade certifikat med “mojibake”.
- En stor mängd certifikat fastnade i *Applied* istället för kortare eller längre tid
- Läget är bättre nu men vi ser fortfarande fördröjningar
-
- Felanmäl vid problem, eskalera via SUNET om det behövs

SUNET

Kommande: DCV via HTTP/HTTPS

CA/B-forum har förbjudit DCV via HTTP/HTTPS att användas för annat än exakt det namnet man validerat, dvs man får inte längre godkänt för hela domänen.

- Ska gälla från 15/11
- Använd email eller DNS för DCV framöver
- Vi arbetar med de tre organisationerna som använt HTTP/HTTPS-validering i SUNET TCS för att lösa övergång

SUNET

Kommande: L bort

Det har varit problem för TCS, Sectigo, certifikatvärlden att enas om vilka värden som är OK för namndelen L (Locality). För att minska risk för problem och revokeringar kommer Sectigo sluta använda L och istället alltid ha med ST (State/Province) där det finns mera strikta regler om vad som är OK.

- Inte ett problem för oss i stort - vi har vettiga ST-värden redan (länsnamn)

SUNET

Kommande: L bort för IGTF-certifikat

Ändringen är mera problematisk för IGTF-servercertifikat (grid-servercertifikat) där alla namn ska vara i ASCII, och där ST för alla våra medlemmar innehåller “län”.

- Diskussioner pågår mellan GÉANT och Sectigo om hur de ska lösa detta. Huvudspåret just nu ett extra ST-fält för ASCII-variant, motsvarande det vi redan har för organisationsnamnet.

SUNET

Kommande: OU bort

Under det kommande året kommer OU att fasas ut på grund av de problem som finns med att validera detta.

- Sectigo har lovat information i tid om ändringarna

SUNET

Frågor?
Kommentarer?

SUNET

Praktiska råd: certifikat-typer

Använd rätt slags OV-servercertifikat

- GÉANT OV multidomain för vanliga
- IGTF-variant bara där man behöver “grid-kompatibilitet”

Låt bli EV-servercertifikat

- En av våra medlemmar använder detta. Deras erfarenhet är inte smärtfri
- Begränsat värde jämfört med OV i praktikten

SUNET

Praktiska råd: fördröjda certifikat

När certifikat är kvar i Applied längre än ni tycker är rimligt:

- Kontrollera att ni har gjort DCV för domänen efter databasmigreringen
- Kontrollera att det inte finns CAA-post i DNS som hindrar utfärdande
- Felanmäl till Sectigo via supportformulär
- Kontakta tcs@sunet.se med case-nummer (samt ordernummer och CN) om/när ni behöver eskalera för snabb hantering

SUNET

Praktiska råd: felanmälan till Sectigo

- Använd https://sectigo.com/support-ticket
- Oftast är Validation Support - Certificate Validation rätt
- Ordernummer skrivs in i rätt fält (vid ärende om flera certifikat, skriv viktigaste ordernummer i fältet och skriv alla i fritextrutan
- Skriv att ni är en del av SUNET TCS och använder SCM på https://cert-manager.com/customer/sunet
- Beskriv problemet, t.ex. “The following certificates are stuck in Applied instead of being issued. Please issue them or tell us what we need to do.”

SUNET

Praktiska råd: kontakt med SUNET TCS

Många av er skickar epost direkt till Kent. Det är OK för att diskutera frågor, långsiktigare saker osv, men om det finns en förväntan om att SUNET TCS ska göra något (t.ex. eskalera ett ärende hos Sectigo) eller ni vill ha svar fort, så ska ni använda tcs@sunet.se (som går till SUNET Jira).

- Använd inte tcs@rt.sunet.se som går till SUNETs äldre ärendehanteringssystem.

SUNET

Praktiska råd: SUNET Wiki

Glöm inte bort guiden på

https://wiki.sunet.se/display/TCS/SUNET+TCS+2020-+Information+for+administrators

Om något du ser där är inaktuellt eller fel, kontakta tcs@sunet.se så vi kan uppdatera.

SUNET

Frågor?
Kommentarer?

SUNET

Framtiden: det blir inte smidigare

Om vi extrapolerar det vi sett de senaste åren och tittar i kristallkulan:

-
- Det kommer fortsätta ske ändringar baserat på CA/B-forum-beslut, incidenter osv som det är svårt för er, oss, GÉANT och Sectigo att ta höjd för i god tid

- Giltighetstider kan komma att reduceras ännu mer

SUNET

Framtiden: automatisera mera

Fundera på vad som fungerar för er organisation för att hantera detta. För många är vägen framåt att automatisera hanteringen mera.

SUNET

Framtiden: automatisera mera

Vägar framåt:

- Sectigos API
- ACME hos Sectigo
- Let’s Encrypt

Kommande erfarenhetsutbyte om detta!

SUNET

Frågor?
Kommentarer?

SUNET

Ge oss feedback!

- Vad tyckte du om detta pass?
- Vad är ditt intryck av höstens Sunetdagar i sin helhet?
- Har du någon annan åsikt du vill dela med dig av?

https://sunet.artologik.net/sunet/sunetdagarnaHT21

SUNET