



SUNET

SUNET TCS - våren 2022

Agenda

- Status
 - tidigare
 - pågående
 - kommande
- Praktiska råd
- Automatisering
 - presentationer från TCS-medlemmar

Tidigare

Prestandaproblem i SCM vid vissa tillfällen

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

SHA384-signaturer

- Finns rapporter om äldre system som inte klarar detta
- Vi har nu möjlighet att utfärda servercertifikat med SHA256

ÅÄÖ-fördröjningar

- Vi ser inte längre fördröjningar eller problem direkt relaterade till detta (som vi diskuterade på förra Sunet-dagarna)

Tidigare: 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.

- Använd email eller DNS för DCV framöver
- Vi har arbetat med de tre organisationerna som använt HTTP/HTTPS-validering i SUNET TCS för att lösa övergång

Tidigare: 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 har Sectigo slutat använda L (åtminstone vid ny- eller omvalidering) 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)
- Återstår att lösa för IGTF-servercertifikat om det blir problem

Pågående: autorenew

Vi rekommenderar inte att ni använder autorenew och manuell hantering eftersom det ofta förvirrar mer än det underlättar när ni ändå måste installera certifikaten “för hand”

Vi har också sett tecken på att extranamn (SAN DNS) som lagts till i gränssnittet (inte i CSR som sådant) saknas vid autorenew.

Kommande: OU bort

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

- Sectigo har informerat i god tid (januari 2022) att OU försvinner från certifikat utfärdade från och med 2022-07-01.

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

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.”

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.

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.

Automatisering - erfarenheter

Presentationer från TCS-medlemmar:

- KTH - Enrico Pelletta och Rikard Wärneryd
- UmU - Kenneth Lindberg
- LU - Morgan Persson
- LiU - Ulrik Haugen