

# Nyckelrullning 2016 - Nyckelceremoni

1. **Installation** (dagen innan)
2. **Rigga** (start 8:00)
  - a. Koppla in kortäsare och RNG i APU
  - b. Koppla in konsolsladd till splitter.
  - c. Koppla splitter till skrivare
  - d. Koppla splitter till laptop via USB-serie-adapter
  - e. Installera terminal emulator på laptop
  - f. Anslut laptop till Adobe Connect och initiera skärmdelning av terminal emulator
  - g. Verifiera att skärmdelning och inspelning funkar
  - h. Boota APU
3. **Utrustning**
  - a. 6 nyckelkort och förse med klistermärken.
  - b. 3 USB minnen (2 för kopia på den privata nyckeln, 1 för överföring av certifikatet)
  - c. Ta fram 9 tamperpåsar:
    - i. 6 påsar till nyckelkort
    - ii. 2 påsar till USB-minnen
    - iii. 1 påse till APU
  - d. Pärm med loggen för APU
  - e. swamid scriptet hämtat från <https://github.com/SUNET/keykeeper>
4. **Nyckelgenerering** (startar 10:00)
  - a. Boota APU
  - b. Kontrollera slumptalsgenerator

```
# swamid ent
```

- c. Starta nyckelgenereringsprocessen

```
# swamid new
```

- d. Under genereringen kommer scriptet fråga efter 6 nyckelkort. Mata in ett kort i taget (vid prompt)
- e. Scriptet visar fingerprint på publika nyckeln. Alla som vill tar en bild.
- f. Scriptet testar nyckelkorten - välj ut 3 slumpmässiga kort
- g. Scriptet dekrypterar den privata nyckeln och startar ett under-skal. Verifiera den privata nyckeln genom att köra följande två kommandon och verifiera okulärt att output matchar.

```
# swamid verify
```

- h. Lägg varje kort i en plastpåse som förseglas. Varje påses serienummer noteras i loggen. Påsarna delas ut till följande personer: Leif, Valter, Pål, Björn, Fredrik, Eskil.
- i. Boota om APU
- j. Nyckelgenereringen är avslutad

5. **Backup**
  - a. Boota APU
  - b. Starta backup-processen:

```
# swamid backup
```

Scriptet promptar efter ett USB minne. Kör backup 2 ggr. När backup är klar, läggs varje USB-minne i var sin påse som förseglas. Påsarna placeras i kassaskåpen på Nordunet, Kastrop (KAS) och hos SUNET på Tulegatan (TUG). Påsarnas serienummer noteras i loggen.

6. **Export**
  - a. Starta export-processen:

```
# swamid export
```

Scriptet kommer att prompta efter ett USB minne. När exporten är klar verifieras innehållet på USB-minnet på valfri laptop varifrån den publika nyckeln läggs upp på mds.swamid.se tillsammans med information om den nya nyckelns fingerprint.

7. **Avslut**
  - a. Gör shutdown på APU
  - b. Lägg APU i en påse som förseglas och placeras i kassaskåpet på TUG. Notera påsens serienummer i loggen.

## Inspelning av nyckelceremonin

- [Inspektion av nyckelceremonin \(Youtube\)](#)
- [Inspektion av nyckelceremonin \(Adobe Connect\)](#)

# Resultat

[nyckelgenerering-logg.txt](#)

Det nya certifikatet:

- SHA256 fingerprint: **A6:78:5A:37:C9:C9:0C:25:AD:5F:1F:69:22:EF:76:7B:C9:78:67:67:3A:AF:4F:8B:EA:A1:A7:6D:A3:A8:E5:85**
- Subject: **C=SE, ST=Stockholm, L=Stockholm, O=SUNET, OU=SWAMID, CN=SWAMID metadata signer v2.0**
- Expire: **Dec 6 09:28:20 2036 GMT**
- [md-signer2.crt](#), <https://mds.swamid.se/md-signer2.crt>