Juurivarmenneprojektin esittely sidosryhmille

Jari Pirinen
Varmenteiden tuoteomistaja
Digi- ja väestötietovirasto
30.09.2021

DIGI- JA VÄESTÖTIETO-VIRASTO

Sisältö

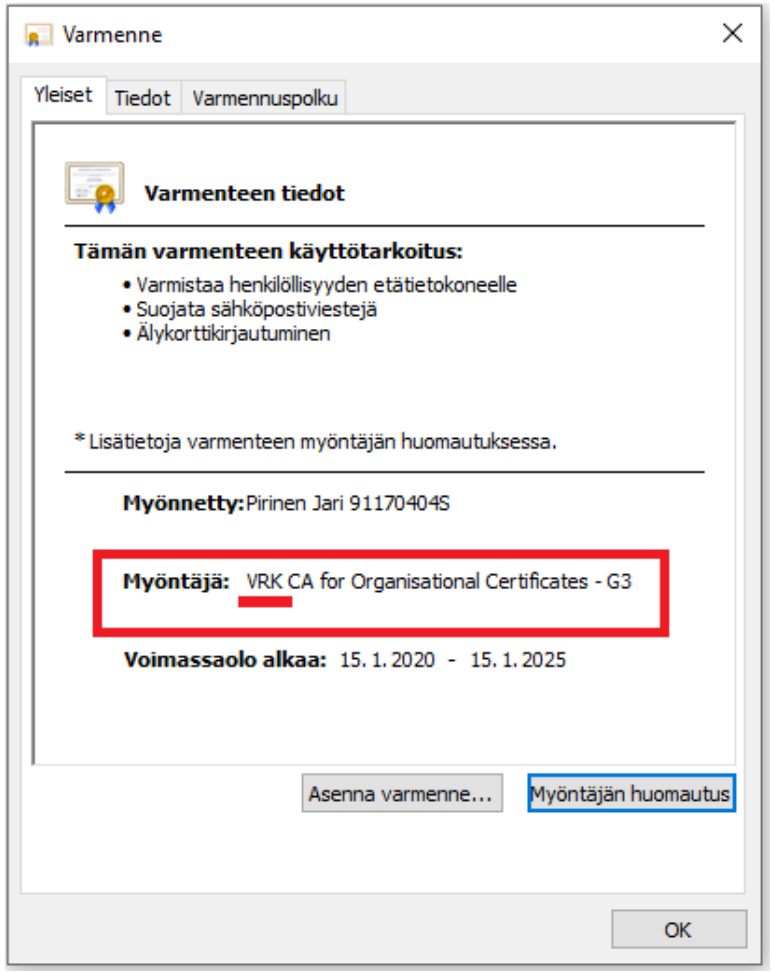
1. Projektin tausta ja tavoitteet
2. Nykytila ja tuleva uudistus
3. Uudet varmennehierarkiat
4. Projektin tilanne
5. Vaikutukset sidosryhmiin
6. Aikaa kysymyksille

TAUSTA JA TAVOITTEET

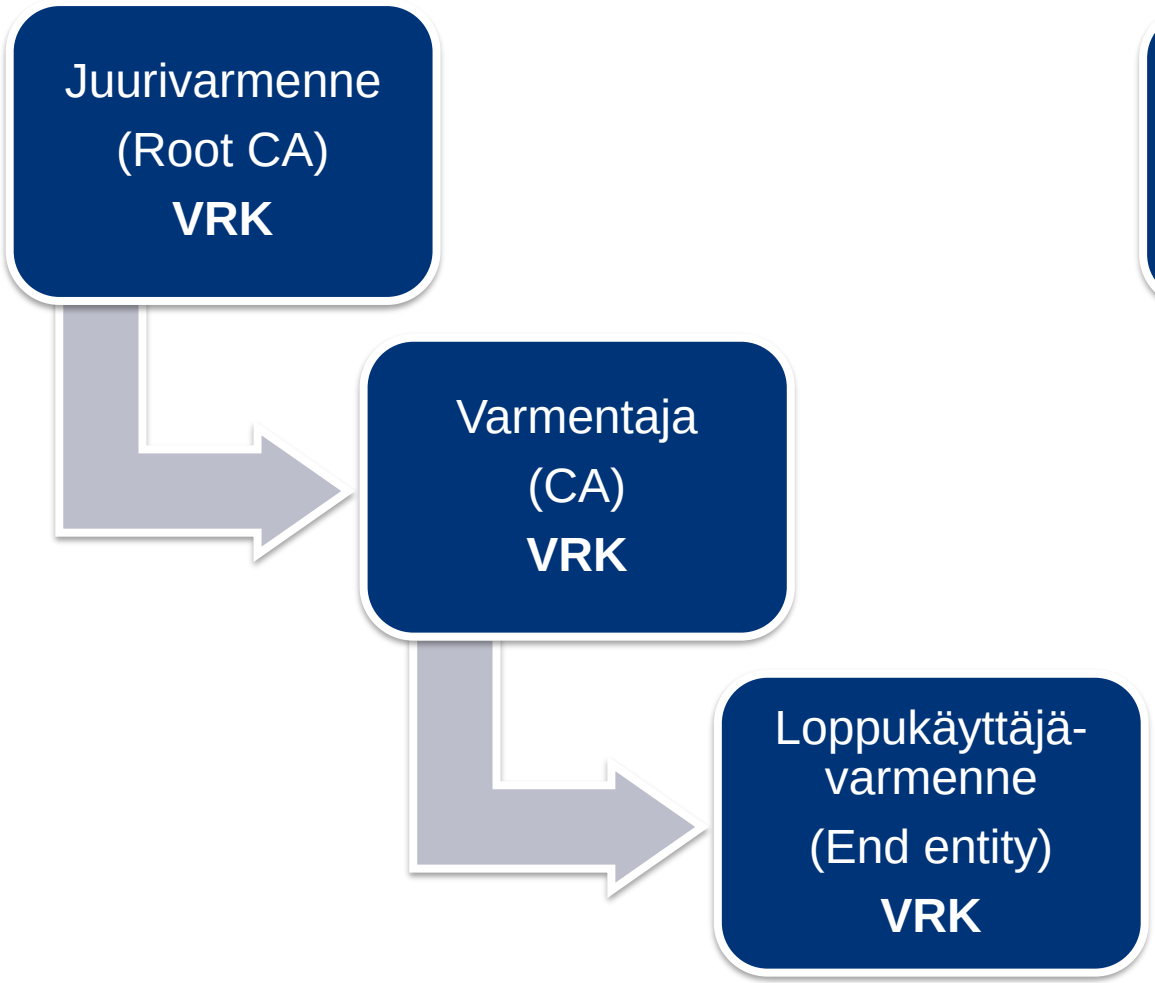
- DVV aloitti toimintansa 1.1.2020.
- Varmennehierarkia on edelleen aiemman viraston eli VRK:n nimissä, joten **uudet varmenteet myöntävänä tahona näkyy tänäkin päivänä edelleen VRK**.
- eIDAS-auditoijamme on antanut varmennehierarkian uudistamiselle **siirtymäajan, joka päättyy kesällä 2022**.
- Juurivarmenneprojekti uudistaa varmennehierarkian DVV:n nimiin.
- Projekti sisältää myös varmennehierarkian auditoinnin ja juurivarmenteiden jakelun.

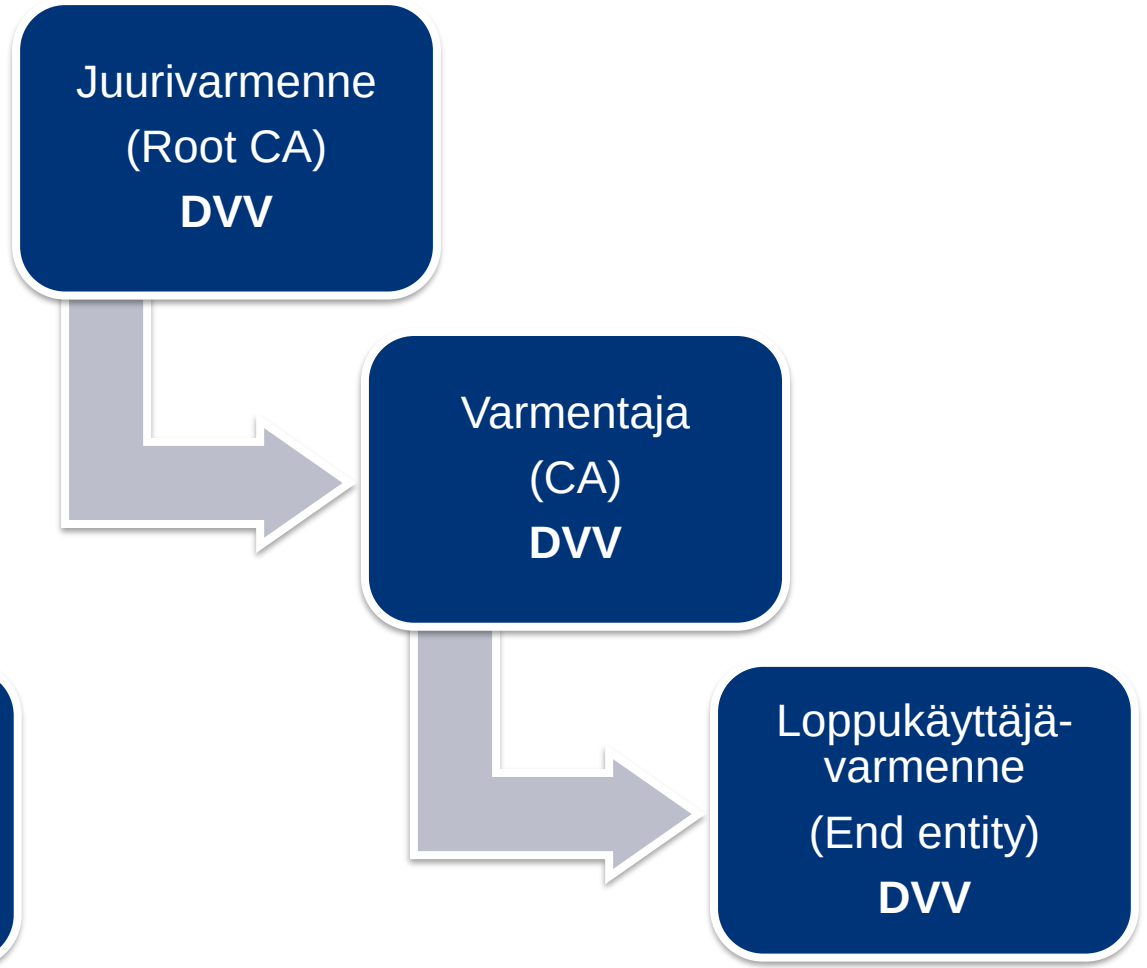
MYÖNTÄJÄN NIMI VARMENTEESSA

Varmenteiden luonteeseen kuuluu, ettei niitä pysty myöntämisen jälkeen enää muokkaamaan miltään osin, vaan koko varmentajahierarkia (*juurivarmenne – CA-varmentajat – loppukäyttäjän varmenne*) täytyy luoda uusiksi nykyisen rinnalle.

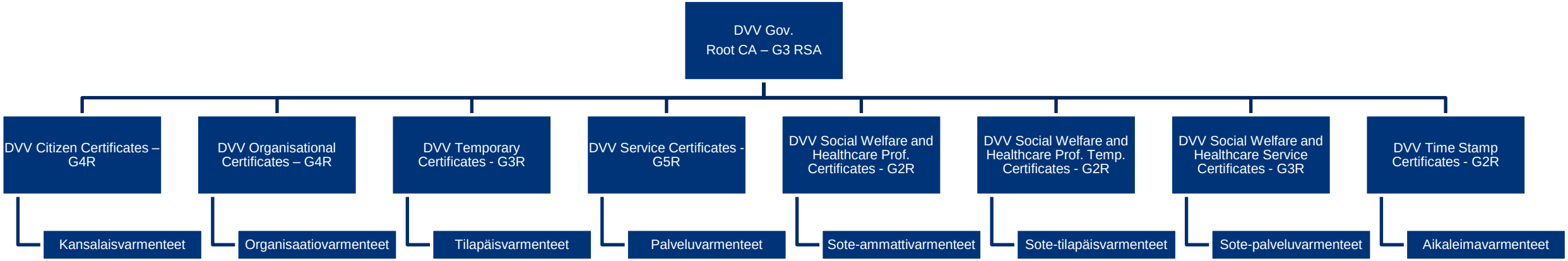


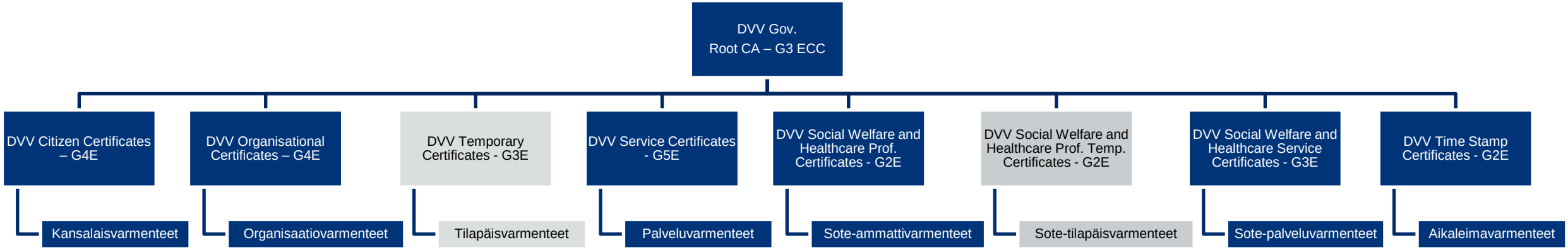
VARMENNEHIERARKIA NYKYINEN / UUSI





DVV:N UUDET G3-VARMENNEHIERARKIAT





PROJEKTIN TILANNE

= Virstanpylväs (Milestone)

Nyt

MAALIS | HUHTI | TOUKO | KESÄ | HEINÄ | ELO | SYYS | LOKA | MARRAS | JOULU | TAMMI | HELMI

VAIHE 1
Aloitus

- Projektin asettaminen
- Projektiryhmän asettaminen
- Valmistelevat työt

VAIHE 2
Tekninen toteutus

- Juurivarmenteiden luominen (**M1**)
- Varmentajien luominen (**M2**)
- Inframuutokset (**M4**)
- Varmennepolitiikat
- Tiedotus sidosryhmille

VAIHE 3
Regulatoriset hyväksynnät

- eIDAS-auditointi (**M3**)
- Traficom-hyväksyntä (**M5**)
- EU-komission hyväksyntä (**M6**)
- CA/B Forum & Microsoft Trusted Root Program –hyväksyntä (**M7**)
- Tiedotus sidosryhmille

VAIHE 4
Tuotannon aloitus

- Uudet varmentajat tuotantoon porrastetusti (**M8-M9**)
- Muutosilmoitus Traficomille
- Tiedotus sidosryhmille

VAIKUTUKSET SIDOSRYHMIIN

- Ennen kuin uudet varmentajat tulevat tuotantoon (joulukuu 2021 … helmikuu 2022), on kaikkien DVV:n varmenteita hyödyntävien tahojen asetettava ne luotetuiksi työasemiinsa ja tietojärjestelmiinsä.

- Työasemien varmenneluottamus asetetaan yleensä keskitetysti AD:ssa.
  - Olkaa yhteydessä omaan tietohallintoonne.
  - Microsoftin asiakasohje uuden CA:n lisäämiseksi AD:ssa.

- Tietojärjestelmien osalta luottamuksen asettaa ko. tietojärjestelmää ylläpitävä taho.
  - Olkaa yhteydessä käyttämienne tietojärjestelmien toimittajiin/ylläpitäjiin.

- Uudet juuri- ja CA-varmenteet ovat ladattavissa: https://dvv.fi/ca-varmenteet

VAADITTAVAT UUDET CA:T SEKTOREITTAIN

- **Sote-sektorin** tulee asettaa vähintään nämä uudet varmentajat luotetuiksi:
  - Juurivarmenteet: DVV Gov. Root CA – G3 RSA ja […] ECC
  - Sote-ammattikortit: DVV Social Welfare and Healthcare Prof. Certificates - G2R ja […] G2E
  - Sote-ammattilaisen varakortit: DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R
  - Sote-henkilöstökortit: DVV Organisational Certificates - G4R ja […] G4E
  - Henkilöstön varakortit: DVV Temporary Certificates - G3R
  - Sote-palveluvarmenteet: DVV Social Welfare and Healthcare Service Certificates - G3R ja […] G3E

- **Muut kuin sote-sektori** asettavat vähintään nämä uudet varmentajat luotetuiksi:
  - Juurivarmenteet: DVV Gov. Root CA – G3 RSA ja […] ECC
  - Organisaatiokortit: DVV Organisational Certificates - G4R ja […] G4E
  - Varakortit: DVV Temporary Certificates - G3R
  - Palveluvarmenteet: DVV Service Certificates - G5R ja […] G5E

VAIKUTUS AIEMPIIN VARMENTEISIIN

- Uusi varmennehierarkia ei millään tapaa vaikuta aiemmin myönnettyjen varmenteiden tai korttien toimivuuteen.
- Kaikki aiemmin myönnetyt varmenteet toimivat normaalisti voimassaoloaikansa päättymispäivään saakka.
- Varmentajalla on velvollisuus taata jokaisen myöntämänsä varmenteen tilatiedon saatavuus koko varmenteen elinkaaren ajan.

ECC-VARMENTEET

- Uusi ECC-varmennehierarkia mahdollistaa algoritmisiirtymän ECC-varmenteisiin.
  - ECC-varmenteet ovat tietoturvallisempia ja suorituskykyisempiä (60-70% nopeammat tunnistautumis- ja allekirjoitusoperaatiot) kuin nykyiset RSA-varmenteet.
  - Suorituskykyero on merkittävin varakortin yksilöinnissä, joka nopeutuu tuntuvasti.
    - Säästää sekä rekisteröijän että loppukäyttäjän (esim. lääkäri) työaikaa.
  - ECC-käyränä käytetään *secp384r1 (NIST P-384)* läpi koko hierarkian.

- Emme ole lyhyellä tähtäimellä pakottamassa asiakkaitamme siirtymään ECC-kortteihin, vaan algoritmisiirtymän aikataulut sovitaan erikseen. **Lyhyellä aikavälillä nykyiset RSA-korttituotteet siis lähtökohtaisesti siirtyvät Q1 2022 aikana käyttämään uudemman sukupolven RSA-CA:ta.**

- Kela tiedottaa erikseen ECC-käyttöönoton aikataulusta Kanta-palveluissa.

ECC-TESTIKORTTIEN TILAAMINEN

- DVV:llä on jo keväästä 2021 lähtien ollut tarjolla ECC-testikortteja, mutta ne on tuotettu hybridivarmenteilla (CA:n nykyisellä RSA-avaimella allekirjoitettu ECC-avain).

- Uuden ECC-hierarkian (*DVV TEST Root CA – G3 ECC*) mukaiset testikortit ovat loka-marraskuun aikana tulossa tilattaviksi verkkoasioinnistamme https://asiointi.dvv.fi/.
  - Tiedotamme erikseen, kun testikortit ovat tilattavissa.
  - Kirjoittakaa testikorttitilauksen kommenttikenttään, että haluatte tilata uuden CA:n ECC-testikortteja.

- Suosittelemme varsinkin sote-sektorin ICT-toimijoita testaamaan ECC:n toimivuutta.

Kysymyksiä ja keskustelua

DIGI- JA VÄESTÖTIETO-VIRASTO