Palveluvarmenteiden tekniset tiedot

Asiakasohje

26.2.2024

Palveluvarmenteiden tekniset tiedot

Sisällysluettelo

1 Yleistä Digi- ja väestötietoviraston palveluvarmenteista

Digi- ja väestötietoviraston (DVV) myöntämät palveluvarmenteet ovat ohjelmistovarmenteita, joilla varmennetaan palveluntarjoajan palvelin tai palvelu.

Palveluvarmenteet perustuvat X.509 standardiin ja niiden avulla on mahdollista toteuttaa selaimen ja palvelimen tai kahden palvelimen välille SSL/TLS-suojattu tietoliikenne.

DVV on ainoa suomalainen varmentaja, joka tarjoaa virallisesti EU-hyväksyttyjä QWAC-varmenteita (Qualified website authentication certificate).

Kaikista palveluvarmenteista on saatavilla myös testiympäristöihin tarkoitetut testivarmenteet, pois lukien sähköpostivarmenteet. Testivarmenteen tietosisältö on sama kuin varsinaisen tuotantovarmenteen.

DVV ei myönnä varmenteita sisäverkkoon eikä myöskään wildcard-varmenteita. Digi- ja väestötietovirasto ei enää myönnä palvelinvarmenteita tai soten palvelinvarmenteita pelkän IP-osoitteen perusteella 15.9.2023 alkaen. Tämän johdosta varmennehakemuksessa on oltava joko domain-nimi tai domain-nimi ja IP-osoite.

Tämän lisäksi DVV ei myönnä 15.9.2023 alkaen palveluvarmenteita, jotka sisältävät sähköpostiosoitteen. Tämä muutos ei vaikuta sähköpostivarmenteisiin, jotka ovat palvelinvarmenteesta erillinen varmennetyyppi.

Valmis palveluvarmenne toimitetaan sähköpostitse hakemuksella määriteltyyn tekniseen yhteissähköpostiin sekä tekniselle yhteyshenkilölle DER ja PEM-tiedostomuodoissa.

2. Palveluvarmennetuotteiden tekniset kuvaukset

Tässä dokumentissa kuvataan lyhyesti Digi- ja väestötietoviraston palveluvarmenteiden tekniset määreet.

2.1 Palvelinvarmenne

Digi- ja väestötietovirasto on ainoa suomalainen varmentaja, joka tarjoaa virallisesti EU-hyväksyttyjä QWAC-varmenteita (Qualified website authentication certificate).

Palvelinvarmenteen avulla verkkopalvelun käyttäjä voi varmistua palvelun tarjoajan aitoudesta. Palvelinvarmenteet mahdollistavat myös palvelimen ja sen käyttäjän välisen tietoliikenteen salaamisen.

Palveluväylän käyttöä varten tarvittavat KaPa autentikointivarmenteet tilataan CSC-Tieteen tietotekniikan keskus Oy:n kautta.

Palvelinvarmenteen tekniset tiedot:

CN (common name)	Domain tai IP osoite	Huomaa että mikäli CN kentässä on IP-osoite, tulee SAN kentästä löytyä vähintään yksi domain
SerialNumber	Ei pakollinen kenttä sallittu tietosisältö on organisaation y-tunnus	Poikkeus: Tullin suoratullausta varten tähän kenttään tulee Tullille EDI-hakemuksessa ilmoitettu VAT/ EORI.
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 3. Nämä voivat olla joko IP-osoitteita tai domainnimiä.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates G5R tai G5E Testivarmenteet: DVV TEST Certificates G2R tai G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.2 Järjestelmäallekirjoitusvarmenne

Järjestelmäallekirjoitusvarmenteella allekirjoitetaan sähköisesti sellaiset asiakirjat, joita ei allekirjoiteta henkilövarmenteilla.

Palveluväylän käyttöä varten tarvittavat KAPA järjestelmäallekirjoitusvarmenteet tilataan CSC-Tieteen tietotekniikan keskus Oy:n kautta.

CN (common name)	Järjestelmän nimi (esim. potilastietojärjestelmä)	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	Organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	Kenttä ei ole sallittu järjestelmäallekirjoitusvarmenteissa	
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates G5R tai G5E Testivarmenteet: DVV TEST Certificates G2R tai G2E	
Key Usages	Digital Signature NonReputation	
Extended Key Usages	-	
Key length, hash	Avainpituus RSA on vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.3 VTJ-rajapinnan asiakasvarmenne

VTJ-rajapinnan asiakasvarmenne on varmenne rajapinnan asiakaskäyttöä (client) var ten DVV:n omille VTJ-asiakkaille.

CN (common name)	Järjestelmän nimi	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	Organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	Vapaaehtoinen kenttä: DNSname1 DNSname2 DNSname3	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 3. Nämä voivat olla IP-osoitteita tai domain-nimiä.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates G5R tai G5E Testivarmenteet: DVV TEST Certificates G2R tai G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.4 Leimavarmenne ja leimapalvelu rajapintavarmenne

DVV tarjoaa leimapalvelun ja testileimapalvelun. Leimavarmenteita ja leimapalvelun rajapintavarmenteita myönnetään vain leimapalvelun ja testileimapalvelun käyttöönottajalle. Lue lisää: linkki leimapalvelun sivulle.

2.5 Sähköpostivarmenne

Sähköpostivarmenne on tarkoitettu organisaatioiden käytössä olevien, yhteiskäyttöisten sähköpostiosoitteiden varmentamiseen. Sähköpostivarmenteen avulla voit vastaanottaa salattuja viestejä ja allekirjoittaa lähtevät viestit. Organisaation sähköpostiosoitteeseen saapuneet salatut viestit avataan sähköpostivarmenteen avulla.

CN (common name)	Sähköpostilaatikkoa kuvaava nimi kuten esim. ”yrityksen nimi” tietohallinnon	
SerialNumber	organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	eMail	Huomaa että DVV tuottaa sähköpostivarmenteita vain yhteiskäytösiin sähköposteihin jonka loppuosan domain ei organisaation oma.
CA (intermediate CA / sub-CA)	DVV Enterprise Certificates	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	eMail protection	
Key length, hash	Avainpituus on 2048 tai 4096 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Sähköpostivarmenne on tiedostopohjainen, eikä sen käyttämiseen ei tarvita kortinlukijoita tai erillisiä ohjelmistoja. Sähköpostivarmenne toimii yleisemmissä S/MIME-viestejä tukevissa sähköpostiohjelmissa kuten Internet Explorer -selaimessa.

Sähköpostivarmenteet ovat PKCS#12-formaatissa.

2.6 Soten palvelinvarmenne

Kanta-palvelujen käyttäjäksi liittyvä organisaatio tarvitsee palvelinvarmenteet eReseptin ja eArkisto-palveluiden käyttämistä varten. Palvelinvarmenne tarvitaan suojaamaan tietoliikenneyhteys (TLS-suojattu) liittyvän organisaation palvelimen ja Kanta-palvelimien välille.

CN (common name)	Domain tai IP osoite	Huomaa että mikäli CN kentässä on IP-osoite, tulee SAN kentästä löytyä vähintään yksi domain
SerialNumber	Kanta-koodiston mukainen OID	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max 3. Nämä voivat olla IP-osoitteita tai domain-nimiä.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates G3R tai G3E Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs G3R tai G3E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.7 Soten järjestelmäallekirjoitusvarmenne

Kanta-palvelujen potilastiedon arkiston käyttäjiksi liityttäessä tarvitaan järjestelmäallekirjoitusvarmenne.

Järjestelmäallekirjoitusvarmenteella allekirjoitetaan sähköisesti sellaiset asiakirjat, joita ei allekirjoiteta terveydenhuollon henkilövarmenteilla.

CN (common name)	Järjestelmän nimi, esim. potilastietojärjestelmä	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	Kanta-koodiston mukainen OID	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	ei sallittu kenttä järjestelmäallekirjoitusvarmenteissa	
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates G3R tai G3E Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs G3R tai G3E	
Key Usages	Digital Signature NonReputation	
Extended Key Usages	-	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.8 Hyvinvointisovellusvarmenne

Sosiaali- ja terveydenhuollon palvelinvarmenne, joka myönnetään hyvinvointisovellus ten sanomaliikenteen suojaamiseksi. Kyseessä ovat esim. mobiilisovellukset joilla käyttäjät keräävät henkilöstä terveystietoja ja välittävät niitä eteenpäin Kelan Omakantaan hyödynnettäväksi.

CN (common name)	Domain tai IP osoite	Huomaa että mikäli CN kentässä on IP-osoite, tulee SAN kentästä löytyä vähintään yksi domain
SerialNumber	Kanta-koodiston mukainen OID	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max 3. Nämä voivat olla IP-osoitteita tai domain-nimiä.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates G5R tai G5E Testivarmenteet: DVV TEST Certificates G2R tai G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).