

Varmennetyyppi	Käyttötarkoitus	SAN- lukumäärä
Standard	Web-palvelimet, palomuurit, kuormantasaajat, yksittäiset palvelimet ja palvelut.	1kpl
Advantage	Web-palvelimet, AD FS federointi, kahden domainin/palvelun varmentaminen ja salaaminen samalla varmenteella, lisänä ECC salausavain.	2 kpl
Wildcard	Alidomainien suojaus. Web-palvelimet, palomuurit, kuormantasaajat, yksittäiset palvelimet.	suositus max. 250kpl
OV Multi-Domain	Usean domainin suojaaminen yhdellä varmenteella. Web-palvelin, palomuurit, kuormantasaajat, palvelimet ja palvelut.	4 kpl (lisä SAN- paikoilla max. 250kpl)
EV Multi-Domain	Verkkokauppojen, pankkien, vakuutus- ja julkishallinnon tai muun korkean tietoturvan palveluiden varmentamiseen.	2 kpl (lisä SAN- paikoilla max. 250kpl)

Varmennetyyppi	Käyttötarkoitus	SAN- lukumäärä
Qualified Web Authentication (PSD2QWAC ja eIDAS QWAC) Qualified Seal (QSealC ja PSD2 QSealC) Lue lisää	Qualified Website Authentication- ja Qualified Electronic Seal-varmenteet autentikointiin, datan salaamiseen sekä muuttumattomuuden todentamiseen. PSD2-, ja eIDAS -standardien mukainen.	1 kpl (lisä SAN-paikoilla max. 250kpl)
Code Signing Certificate(OV/EV)	Koodin allekirjoittaminen. Aikaleimaus, tiedoston/koodin muuttumattomuuden todentaminen sekä allekirjoittajan tunnistaminen. Saatavilla sekä OV- ja EV-tasoisena. Huom! Windows 10-ajureiden allekirjoittamiseen tarvitaan EV-tasoinen Code Signing -varmenne.	-

Varmennetyyppi	Käyttötarkoitus	SAN- lukumäärä
Document Signing Certificate Lue lisää	Dokumenttien digitaalinen allekirjoittaminen. Aikaleimaus, dokumentin muuttumattomuuden todentaminen, sekä allekirjoittajan tunnistaminen. Yhteensopiva Adobe PDF- ja Microsoft -asiakirjojen kanssa. Kiiistämättömyys voimassa asiakirjan elinkaaren ajan.	-
S/MIME-Certificate	Sähköpostin salaust sekä digitaalinen allekirjoitus.	-
Verified Mark Certificate	Asiakasviestinnän selkeyttämiseen sekä brändinäkyvyyden parantamiseen. Yrityksen rekisteröity logo tunnisteena sähköposteissa.	-

Certificate type	Usage	SAN-count
Standard	Web servers, firewalls, load balancers, individual servers and services.	1 pcs
Advantage	Web servers, AD FS federation, authentication and encryption of traffic between two domains, with added ECC encryption key.	2 pcs
Wildcard	Subdomain protection, Web-servers, firewalls, load balancers, individual servers.	recommendation max. 250 pcs
OV Multi-Domain	Securing multiple domains with a single certificate. Web server, firewalls, equalizers, servers and services.	4 pcs (with extra SAN-units max. 250pcs)
EV Multi-Domain	For online stores, banks, insurance and public administration or other high security services.	2 pcs (with extra SAN-units max. 250pcs)

Certificate type	Usage	SAN-count
Qualified Web Authentication (PSD2QWAC and eIDAS QWAC) Qualified Seal (QSealC and PSD2 QSealC) Read more	Qualified Website Authentication and Qualified Electronic Seal -certificates for authentication, data encryption, and tamper-proofing. Based on the EU's eIDAS regulations and the finance sector's Payment Services Directive 2 (PSD2)	1 pcs (with extra SAN-units max. 250pcs)
Code Signing Certificate(OV/EV)	Certificate for code signing. Timestamping, file/code integrity verification and signer identification. Available in both OV and EV levels. Note: signing Windows 10 drivers requires an EV level Code Signing Certificate.	-

Certificate type	Usage	SAN-count
Document Signing Certificate Read more	Digital signing of documents. Timestamping, document integrity verification, and signer identification. Compatible with Adobe PDF- and Microsoft-documents. Indisputability valid for the life of the document.	-
S/MIME-Certificate	Email encryption and digital signature.	-
Verified Mark Certificate Read more	To improving customer communication and brand visibility. Company's registered logo as an identifier in sent emails.	-

Käyttötarkoitus	Varmenteen nimi ja kuvaus	SAN- lukumäärä
Web-palvelimet, palomuurit, kuormantasaajat, yksittäiset palvelimet. Julkisesti luotettu varmenne, jonka ominaisuuksista käy ilmi myös palvelimen/ palvelun omistaja.	Entrust Standard varmenteella suojaat verkkosivujesi liikenteen yksinkertaisesti ja helposti. Selain/asiakas tunnistaa varmenteen perusteella palvelimen luotettavasti ja varmenteen avulla luodaan salattu yhteys näiden välille. Entrust Standard varmenteella turvaat yhden domainin palvelut ja liikenteen (example.com ja www.example.com). Joustava uudelleen luonti (reissue): jos jotain meni pieleen tai varmenne täytyy muusta syystä uusia, voidaan varmenteelle tehdä reissue-toiminto aina 60 päivää ennen varmenteen voimassaolon päättymistä, esim.uudella CSR:llä.	1+1 kpl esim: www.example.com ja example.com.
Web-palvelin, AD FS federointi, kahden domainin välisen liikenteen varmentaminen.	Entrust Advantage suojaa kaksi domainia samalla varmenteella. Se soveltuu myös palvelinten välisen liikenteen suojaamiseen, esimerkiksi AD FS (Active Directory Federation Service), koska sillä voidaan vaatia myös selaimen tunnistus. Entrust Advantage sisältää kahden domainin lisäksi oletusdomainin: esim. CN = www.asiakas.fi ja oletuksena mukaan tulee myös SAN = asiakas.fi. Joustava uudelleen luonti (reissue): jos jotain meni pieleen tai varmenne täytyy muusta syystä uusia, voidaan varmenteelle tehdä reissue-toiminto aina 60 päivää ennen varmenteen voimassaolon päättymistä, esim.uudella CSR:llä.	2+1 kpl esim. example.com, www.example.com ja example.



Käyttötarkoitus	Varmenteen nimi ja kuvaus	SAN- lukumäärä
Koko ROOT-domainin varmentaminen yhdellä varmenteella. Web-palvelin, palomuurit, kuormantasaajat, yksittäiset palvelimet. Julkisesti luotettu varmenne, jonka ominaisuuksista käy ilmi myös palvelimen/palvelun omistaja.	Entrust Wildcard suojaa koko root-domainin yhdellä varmenteella. Voit suojata esim. domainin *.asiakas.fi sekä lisädomainit www.asiakas.fi, mail.asiakas.fi jne. Samaan Entrustin varmenteeseen saat myös lisää *-määritteitä, kuten *.portaali.asiakas.fi. Entrust Wildcard sisältää ReKey-ominaisuuden, eli voit luoda samasta varmenteesta duplikaatteja ilman eri veloitusta. Ominaisuuksiltaan markkinoiden joustavin Wildcard, johon saat lisättyä erillismaksusta jopa 250 lisä-SANia. Joustava uudelleen luonti (reissue): jos jotain meni pieleen tai varmenne täytyy muusta syystä uusiksi, voidaan varmenteele tehdä reissuetoiminto aina 60 päivää ennen varmenteen voimassaolon päättymistä, esim.uudella CSR:llä.	Entrust wildcard: Maksimi 250 kpl esim. *.example.com, example.com. Voi sisältää myös toisia wildcardoja, esim. *.palvelut.example.com
Usean domainin varmentaminen yhdellä varmenteella. Web-palvelin, palomuurit, kuormantasaajat, yksittäiset palvelimet. Julkisesti luotettu varmenne, jonka ominaisuuksista käy ilmi myös palvelimen/palvelun omistaja.	Entrust UC Multi-Domain soveltuu esim. Exchange, Lync tai Skype for Business - palvelimien ja -ympäristöjen suojaamiseen. Käytetään muutenkin silloin, kun samalla varmenteella pitää suojata useita domain-nimiä. UC Multi-Domain varmenteella on mahdollista suojata jopa 250 domain-nimeä (esim. autodiscover.ssl-apua.fi, sip.ssl-apua.fi, palvelu1.ssl-apua.fi, www.ssl-apua.fi, ssl-apua.com...). Joustava uudelleen luonti (reissue): jos jotain meni pieleen tai varmenne täytyy muusta syystä uusiksi, voidaan varmenteele tehdä reissuetoiminto aina 60 päivää ennen varmenteen voimassaolon päättymistä, esim.uudella CSR:llä.	4+1 kpl, maksimi 250 kpl esim. example.com, example.fi, esimerkki.com, esimerkki.fi. ja www.example.com. Varmenteen CN= attribuuttia vastaava www. nimi kuuluu varmenteen mukaan.

Käyttötarkoitus	Varmenteen nimi ja kuvaus	SAN- lukumäärä
Extended Validation, eli EV-varmenne on suositeltava web- kauppojen, pankkien, vakuutus- ja julkishallinnon tai muun korkean tietoturvan palveluiden varmentamiseen. Vihreä osoitepalkki, josta näkee suoraan palvelun omistajan nimen	Entrust Wildcard suojaa koko root-domainin yhdellä varmenteella. Voit suojata esim. domainin *.asiakas.fi sekä lisädomainit www.asiakas.fi, mail.asiakas.fi jne. Samaan Entrustin varmenteeseen saat myös lisää *-määritteitä, kuten *.portaali.asiakas.fi. Entrust Wildcard sisältää ReKey-ominaisuuden, eli voit luoda samasta varmenteesta duplikaatteja ilman eri veloitusta. Ominaisuuksiltaan markkinoiden joustavin Wildcard, johon saat lisättyä erillismaksusta jopa 250 lisä-SANia. Joustava uudelleen luonti (reissue): jos jotain meni pieleen tai varmenne täytyy muusta syystä uusia, voidaan varmentelle tehdä reissuetoiminto aina 60 päivää ennen varmenteen voimassaolon päättymistä, esim.uudella CSR:llä.	Entrust wildcard: Maksimi 250 kpl esim. *.example.com, example.com. Voi sisältää myös toisia wildcardoja, esim. *.palvelut.example.com
Koodin allekirjoitus	Entrust Code Signing Certificate on koodin allekirjoittamiseen tarvittava varmenne. Luotettavien ohjelmistojen kehittäminen ja jakelu edellyttää tänä päivänä sitä, että koodi on allekirjoitettu julkisella varmenteella. Code Signing varmenne vaatii aina EV-varmennetun domainin käyttäjälleen, eli korkeimman turvatason varmennuksen. Koodin allekirjoittamiseen on mahdollista saada tokenilla/HSM-laitteella suojattu EV Code Signing varmenne tai OV Code Signing varmenne. Tietoturvan kannalta on olennaista, että kone, jolla koodin allekirjoittaminen tehdään, pidetään turvassa ja siihen on pääsy vain niillä henkilöillä, joiden tehtävänä on koodia allekirjoittaa. CA Browser Forum on määritellyt standardiksi, että kaikki Code Signing varmenteet tulee olla ns. hardware-suojattuja. Vaikka edellämainittu tapa on OV Code Signing varmenteen kanssa mahdollinen, nämä varmenteet toimitetaan oletusarvoisesti tokenin kera. Mikäli varmennetta kuitenkin halutaan käyttää ilman tokenia, on käyttäjän otettava vastuu varmenteen turvallisesta käytöstä itselleen. Varmenteen toimittajalla on oikeus revokoida varmenne, mikäli väärinkäytöksiä havaitaan. Tokenilla suojattu versio ei toimi ilman, että token on allekirjoitushetkellä käytössä	2+1 kpl Ei sisällä SANEja.

Käyttötarkoitus	Varmenteen nimi ja kuvaus	SAN- lukumäärä
Dokumenttien allekirjoitus	Entrust Document Signing Certificate on tarkoitettu erilaisten dokumenttien allekirjoittamiseen, eli todistamaan sen, kuka dokumentin on tuottanut. Näitä käytetään virallisten dokumenttien yhteydessä, kun halutaan varmistaa dokumenttien oikeellisuus ja se, ettei niitä ole muokattu ulkopuolisten toimesta.	Ei sisällä SANEja.
Sähköpostien salaus ja allekirjoitus	Entrust S/MIME-Certificate on tarkoitettu sähköpostiliikenteen salaamiseen ja allekirjoittamiseen. Tätä varmennetta käytetään hyvin yleisesti sähköpostiliikenteen suojaamiseen. S/MIME on standardi, joka soveltuu käytettäväksi useimpien sähköpostiohjelmistojen kanssa.	Ei sisällä SANEja.

