



Korkean käytettävyyden varmennepalvelujärjestelmä hallinnoituna kokonaispalveluna

PALVELUKUVAUS

Liiketoiminnan kriittisten tietojen suojaaminen, niihin liittyvien prosessien tehostaminen ja uuden liiketoiminnan mahdollistaminen ovat tietoturvan tärkeimmät päämäärät

Hallinnoitu PKI palvelu säästää rahaa ja aikaa

Käyttääkö organisaatiosi tietoverkkoja tietoturvallisesti liiketoiminnalle tärkeiden tietojen siirtoon ja viestintään? Hyödyntääkö organisaationne tietoverkkojen sisäänrakennettuja suojakeinoja viestinnän turvaamiseksi? Tarvitseeko organisaationne tunnistaa käyttäjät, laitteet tai sovellukset, jolle annetaan pääsy tietojärjestelmiin, tietoverkkoihin ja liiketoiminnan tietovarantoihin? Suojataanko organisaatiossanne käyttäjien etäyhteydet VPN tuotteilla? Mikäli vastaat kyllä, tarvitset kaikkeen tähän varmenteita.

Ulkoista PKI:n tekniset haasteet

Itsessään varmennepalvelujärjestelmän pystyttäminen ei ole nykyteknologioiden kannalta samanlainen suururakka kuin vielä takavuosina, sen sijaan oman varmennepalvelujärjestelmän hallinnointi, ylläpito ja sisällyttäminen eri liiketoimintaprosesseihin on edelleen suuri haaste. Suureksi haasteen tekee se, että PKI-, eli varmennepalvelujärjestelmä koostuu monesta osasta, ominaisuudesta ja toiminnallisuudesta jotka ovat olennaisen tärkeitä järjestelmän toimivuudelle, turvallisuudelle ja luotettavuudelle. Tänä päivänä vain harvalla organisaatiolla kuuluu kaikkien näiden asioiden täydellinen hallinta. Organisaation IT valjastetaan ketteräksi ja liiketoimintavetoiseksi, tehokkaasti johdetuksi prosessiksi tukemaan organisaation kilpailukykyä samalla kun teknologia- ja liiketoimintaympäristöt muuttuvat kiihtyvää vauhtia. Yhä useammin onkin järkevää arvioida miten eri IT-toiminnot voidaan ulkoistaa ja järkipäristää. Nyt on aika arvioida miten myös varmennepalvelujärjestelmän ulkoistus luotettavalle ammattiorganisaatiolle voi tuoda selvää säästöä tietoturva tuottavien prosessien hallinnointiin. Varmennepalvelun ulkoistus on erinomainen vaihtoehto oman kapasiteetin ylläpidon sijaan. Palveluna tuotettu varmennepalvelujärjestelmä ei kuluttaa talon omia IT resursseja, joilla on tärkeä rooli varsinaisen liiketoiminnan tukemisessa ja kehittämisessä.

Hallinnoidulla PKI -palvelulla tuotetaan kustannustehokkaasti organisaation tarpeisiin räätälöidyt varmennepalvelut kaikista korkeimmilla turvallisuus- ja luotettavuuskriteereillä.

Useimmat yritykset ja organisaatiot, jotka ovat suunnitelleet, testanneet, pilotoineet tai ottaneet aikojen saatossa PKI-palveluja jonkin asteiseen käyttöön, ovat huomanneet että PKI-hankkeisiin kuluu vaikeasti ennakoitavan paljon aikaa ja rahaa ilman että varsinaisiin lisäarvokysymyksiin päästään kunnolla edes tarttumaan. Tavanomaisen organisaatio-PKI -järjestelmän laitteisto- ja mahdolliset lisenssikulut vastaavat yksistään jo 60% tuotannossa olevan PKI-järjestelmän kuluista. Toteutusprojektin hinta voi tämän lisäksi muodostua moninkertaiseksi PKI-järjestelmän laitteisto- ja lisenssikustannuksiin verrattuna. Henkilöresurssien hankkiminen, ylläpitäminen, kouluttaminen ja projektityön ylläpito muodostavat niin ikään merkittävän kustannuserän, jota on erittäin vaikea ennakoida ja budjetoida.

Resurssien saatavuuteen (laitteistot, tilat, lisenssit, henkilöstö) liittyvät haasteet voivat olla ratkaistavissa suuressa organisaatiossa. Nopeaan PKI-projektin toteutumiseen, suuruuden tuomiin määrätuihin, varmennepalvelutoiminnan auditoitavuuteen ja sertifiointiin, sekä eri osapuolten luottamussuhteiden hallintaan liittyvät kysymykset asettavat kuitenkin haasteita, joihin suurelta osin organisaatiot eivät pysty vastaamaan nopeasti. Nopeus on kuitenkin yksi tärkeimmistä elementeistä

hyvin palvelevassa PKI-ympäristössä: tilanteet, tarpeet ja vaatimukset muuttuvat nopeasti ja suuren tietoturva-arkkitehtuurin pitäminen ajan tasalla ja tarpeita vastaavana ei ole helppo tehtävä.

PKI-palvelutoiminta on oma erikoisalansa, jossa nopeasti muuttuvat teknologiat, kirjavat liiketoimintaprosessit ja –mallit, sekä monitasoiset turvallisuusvaatimukset yhdistyvät yhdeksi kokonaisprosessiksi. Hallinnoidun PKI-palvelun liiketoimintaidea perustuu siihen, että PKI ulkoistettuna erityisosaajapalveluna mahdollistaa kustannussäästöt niin ajassa kuin resurssitarpeissa ja auttaa organisaatiota kehittämään paremmin, tehokkaammin ja innovatiivisemmin omaa liiketoimintaansa, perustuen korkeaan tietoturvaan, luottamukseen ja sähköisiin prosesseihin.

Mitä BBS:n hallinnoima varmennepalvelujärjestelmä tarjoaa?

BBS:n hallinnoitu PKI tarjoaa yksinkertaisen, nopean ja edullisen tavan tilata ja hallinnoida käyttäjä-, laite- ja sovellusvarmenteita suojatun verkon yli. Varmennetietojärjestelmän asennus, hallinnointi, ylläpito, valvonta ja räätälöinti tuotetaan keskitetysti BBS:n tietoturvasertifioidun korkean turvatason palvelukeskuksesta käsin. Varmenteiden käyttöönotto ei edellytä lainkaan laite- tai järjestelmäinvestointeja tai varmennejärjestelmän toteuttamiseen tarvittavaa asiakkaan oma työpanosta. BBS:n tarjoaman palvelun joustavuus ja laajennettavuus takaa lähes rajattomat mahdollisuudet räätälöidä varmennepalvelu sellaiseksi miksi asiakas sen haluaa. Asiakas saa itse määrittellä kaikki eri politiikat, käytännöt ja turva-asetukset omien tarpeiden ja vaatimusten mukaisesti, kuten varmenteiden avainpituudet, voimassaoloajat, varmenteiden sulk- ja avainten palautuskäytänteet. Luonnollisesti asiakas saa parhaan mahdollisen asiantuntijatuon kaikkien asetusten ja toimintatapojen turvalliseen ja optimoituun määrittelyyn. Varmennettujen identiteettien koko elinkaaren hallinta saadaan täten osaksi asiakasorganisaation normaaleja IT – rutiineja ja tukemaan liiketoimintakriittisiä palveluja kustannustehokkaasti ja saavuttaen korkeimman mahdollisen tietoturvatason ilman suuria ponnistuksia.

Tarjottuihin PKI-palveluihin kuuluu EU:n sähköisen allekirjoituksen direktiivin mukainen laatuvarmennepalvelu (Qualified Certificate Authority), hallinnoitu PKI-palvelutoiminta ja -ympäristö, mobiili sähköisten allekirjoitusten Wireless PKI -palvelukokonaisuus, Multi-ID -tunnistusportaalipalvelu, sähköisten allekirjoitusten workflow-prosessipalvelut sekä sähköisten asiakirjojen pitkän ajan arkistointipalvelu. Näiden lisäksi palveluihin kuuluu Global Validation Service –palvelu rajat ylittävien sähköisten allekirjoitusten riskipohjaiseen tarkistamiseen ja vahvistamiseen. Globaali palvelu tuotetaan yhteistyössä Det Norske Veritasin (DNV) kanssa.

Palveluntarjoaja

Secure Link Oy on uusi suomalainen tietoturva-alan palvelu- ja asiantuntijaorganisaatio, jonka osakkaina ovat Conseils Oy ja XCure Solutions Oy sekä Markus Lehtonen Enterprises Oy. Conseils Oy on 1987 perustettu PKI- ja varmennekorttiratkaisujen ja palvelujen konsultointiin ja hallintaan erikoistunut asiantuntijayritys. XCure Solutions Oy on tietoturvapalveluihin erikoistunut asiantuntijapalveluorganisaatio, joka on perustettu 2006. Markus Lehtonen Enterprises Oy on lukitus- ja verkkoturvallisuus sekä etätunnisteteknologian että identiteettihallinnan ratkaisuja tarjoava palveluyritys, joka on perustettu 2009. Conseils ja XCure sekä MLE ovat toimineet yhteistyössä XCuren perustamisesta lähtien ja sitä ennen samojen henkilöiden kanssa yhteistyössä vuodesta 2001 lähtien.

Olemme asiantuntija- ja palveluyritys, jonka tehtävänä on edustaa, hallinnoida ja organisoida PKI- ja varmennekorttiratkaisuihin liittyviä palveluja. Secure Link tarjoaa yhden Suomen suurimmista PKI- ja varmennepalveluihin erikoistuneista asiantuntija- ja palveluorganisaatioista, jossa toimii yhteensä 10 pitkän linjan sertifioituja tietoturva-asiantuntijoita ja senior-tason konsultteja ja teknisiä asiantuntijoita. Olemme luoneet Suomeen palvelutoiminnan, jossa tuomme paikallisen tuen, ylläpidon, projektihallinnan ja integraatiopalvelut BBS:n PKI-palvelujen tuottamiseksi asiakkaan palveluihin ja järjestelmiin.

Secure Link edustaa Suomessa norjalaisen BBS AS -yhtiön hallinnoituja varmennepalveluja. Päämiehemme BBS on pohjoismaiden suurin kaupallisten PKI-palvelujen tuottaja: BBS tuottaa mm. Norjan, Ruotsin ja Tanskan kansalliset varmennepalvelut, Norjan pankkien BankID -palvelut, sekä useita kaupallisia varmennepalveluja sekä validointipalveluja pohjoismaissa ja Baltiassa, kuten pankkivarmenteet, terveydenhuollon ammattivarmenteet ja mobiilivarmenteet. BBS on hallinnoinut kriittisiä pankkijärjestelmiä Norjassa vuodesta 1972 lähtien ja PKI-järjestelmiä vuodesta 1997 lähtien. BBS:n korttimaksuhallinnan, PKI- ja sähköisten laskujen hallinnan palvelut ovat maailman käytetyimmät infrastruktuuripalvelut omilla saroillaan. BBS:llä on toimipisteet kaikissa Pohjoismaissa sekä Virossa. Suomessa BBS toimii yhteistyökumppani Secure Link Oy:n edustamana sekä itsenäisenä pankkikorttimaksupäätteiden hallintaan erikoistuneena yksikkönä vuodesta 2009 lähtien (entinen Manison Finland Oy) . BBS:llä on PKI -palveluasiakkaita useissa Euroopan maissa, mm. yli 150 pankkia ja pankkiryhmää Euroopassa, kansainvälisiä konserneja, teleliikenneoperaattoreita, julkisen sektorin organisaatioita sekä myös pieniä ja keskusuuria yrityksiä.

1. PKI-palvelun kuvaus

1.1. Yleiskatsaus

Hallinnoitu PKI-palvelu on turvallinen ja samalla edullinen tapa toteuttaa varmennepalvelut: BBS:llä on käytössään yksi maailman turvallisimmista tuotantoympäristöistä, sillä on erittäin suuri asiakaskunta (miljoonia varmenneasiakkaita) ja hyvin suuret tekniset resurssit tuottaa PKI-palveluja tehokkaasti. BBS:n edullisuus perustuu suureen volyymiin ja siihen, että sen tarjoamat PKI-alustat (Entrust, Verizon) ovat täysin BBS:n omistuksessa, jolloin asiakkaat saavat tarvitsemansa palvelut niin joustavasti kuin se on teknisesti ja kaupallisesti mahdollista.

Varmenne, joka sisältää käyttäjän julkisen avaimen sekä identiteettitiedot, luodaan ja hallinnoidaan varmentajan toimesta. Varmentaja käyttää hyväkseen julkisen avaimen salausmenetelmää (PKI) jonka avulla käyttäjät voidaan tunnistaa, tiedot voidaan suojata ja sähköiset asiakirjat ja tapahtumat allekirjoittaa sähköisesti. Varmentajan ja varmenteiden ansiosta voidaan luoda ja ylläpitää luotettavaa viestintää ja tiedonsiirtoa tietoverkoissa.

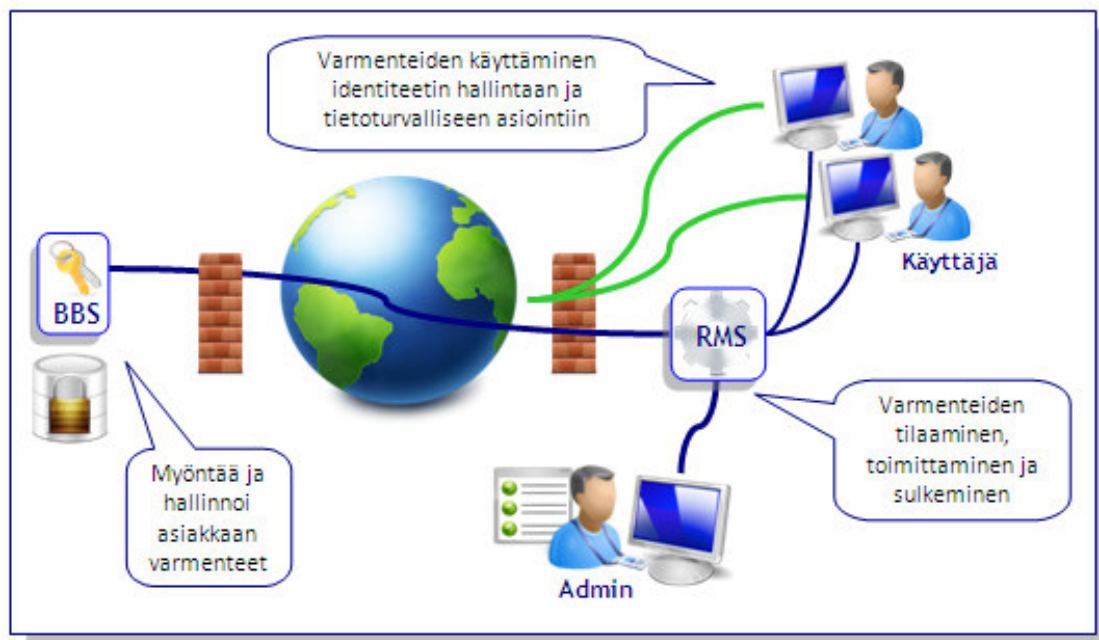
1.2. Hallinnoitun PKI-palvelun sisältö

BBS:n hallinnoiman PKI-palvelun perustana ovat:

- Korkealaatuinen PKI-alusta (Entrust tai Verizon) ja varmennepalvelu
 - Hierarkkinen tai yksitasoinen PKI
 - Varmenteiden hallinta itsepalveluna, sekä Web RA
 - Dedikoidut laadunhallinta- ja testiympäristö asiakasorganisaation käyttöön
 - 2, 3 tai useampi varmenne / käyttäjä
 - CRL-sulkulistapalvelut tai varmenteiden voimassaolon tarkistuspalvelut (perinteinen OCSP tai korkean käytettävyyden Distributed-OCSP)
- Kaikki laitteet ja sovellukset palvelun tuotantoon:
 - Kahdennetut palvelimet
 - Kahdennetut yhteydet
 - CA-lisenssit
 - Validointijärjestelmälisenssit
 - Kahdennetut FIPS-sertifioidut HSM-laitteistot avainten hallintaan
- Taattu palvelutasosopimus (SLA)
 - Palvelutaso: käytettävyyssaste 99.5% - 99.7% (poislukien ennalta sovitut huoltokatkokset)
 - Tuotantovalmius alle kolmessa kuukaudessa
 - Huomioi heterogeenisen käyttöympäristön: sisäinen ja ulkopuolisille tarkoitettu käyttö
 - 24x7 tuki kaikille sopimuksen alaisille palveluille

- Täydellinen dokumentaatio (varmennepoliitikat, varmennekäytännöt, muu dokumentaatio)
- ISO/IEC 27001 tietoturvasertifioitu palveluympäristö ja –tarjoaja
- Säännöllinen tietoturvatarkastus itsenäisen auditoijan toimesta
- Verkkoysteimet
 - Verkkoysteimet tuotetaan internetin kautta, dedikoidun verkon kautta tai näiden yhdistelmänä
 - Kaikki verkkoliikenne ohjataan usean palomuurin läpi ja liikennettä valvotaan erilaisten hyökkäysten estojärjestelmien avulla (IDS ja IPS järjestelmät)
 - Liikenteen kuormitusta tasataan kuormantasaajilla. Kuormantasaajat takaavat korkean käytettävyyden eri toimintahäiriöiden, poikkeustilanteiden ja verkkoruuhan varalta. Palvelu käyttää useaa kuormantasaajaa
 - Kaikki verkkoysteimet ovat moninkertaisia ja vähintään kahdenkertaista. Asiakkaalle tarjottu palvelu ole koskaan ainoastaan yhden tietoliikennepalvelutarjoajan yhteyden varassa
 - Verkot ja PKI-tuotannon tilat on segmentoitu usealle eri turvavyöhykkeelle. Korkeimman turvatason tuotantotilojen verkkoysteimet ovat täysin erotetut muista yhteyksistä

Tarkempi lista PKI-palvelun sisällöstä on annettu Secure Link Oy:n esitteessä ”Managed PKI: Service Content - FI”.



Kuva 1: BBS:n hallinnoitu PKI-palvelu on käytettävissä kaikkialta maailmassa. Palvelu tukee kansainvälisten asiakasorganisaatioiden globaaleja operaatioita joustavasti, skaalautuvasti ja turvallisesti.

1.3.Laadun hallinta ja palveluntarjoajan sertifiointit ja kompetenssit

BBS:n varmennepalvelutuotannossa työskentelee yli 50 kokopäiväistä tietoturva-, tietoliikenne- ja tietotekniikan alojen PKI-ammattilaista. PKI-asiantuntijaorganisaationa BBS on yksi Euroopan

suurimmista toimijoista ja ylivoimaisesti suurin Pohjoismaissa ja Baltiassa. Huomioitavaa on lisäksi se, että BBS on yksi harvoista kaupallisesti kannattavista varmennepalvelun tuottajista koko maailmassa.

1. ISO/IEC 27001 -tietoturvasertifioitu toiminta
2. ISO 9001 laatutoimintasertifiointi
3. PCI-DSS standardin mukainen toiminta
4. ETSI TS 101 456 -mukainen laatuvarmennepalvelutoiminta
5. 60 täysipäiväistä turvatarkastettua ammattilaista vastaamassa palvelutuotannosta
6. Kattavat vakuudet toiminnan jatkuvuudesta ja vahva omistajasitoutuminen (asiakkaina toimivat pankit omistavat BBS:n)
7. Dun & Bradstreet AAA luottoluokitus (2009)

1.4. Secure Link Oy palvelut

Secure Link tuottaa

- RA-rekisteröintipalvelujen ylläpito ja tuki
- BBS:n tuottamien PKI-palvelujen ensimmäisen tason paikallinen ja suomen ja ruotsinkielinen tuki, sekä 2 ja 3 tason tuen eskalointi 24/7 valmiudella.
- Asiakasprojektipalvelut
 - Varmennemääritykset asiakastarpeisiin (varmenneprofiilit, voimassolot, avainpituudet, hierarkiat, jne.)
 - Tekniset määritykset varmenteille ja varmennevälineille (mm. varmenesovellukset, toimikortit, jne.)
 - Varmennehallinnan prosessien määrittely ja toteutus (rekisteröintimenettelyt, PIN- ja PUK-tunnusten hallinta, varmenteiden elinkaaren hallinta)
- Integraatiopalvelut
 - Varmenteiden käyttäminen toimikorteilla, USB-avaimilla tai muilla suojatuilla välineillä, mukaan lukien middleaware tuotteet ja lukijalaitteet
 - Fyysisen ja loogisen tunnistuksen yhdistäminen samalle tunnistusvälineelle
 - Kertakäyttösalanapalvelujen liittäminen
 - Varmenteiden hyödyntäminen identiteetin hallinnan järjestelmissä (federaatio, kertakirjautuminen, provisiointi ja de-provisiointi)
 - Korttien hallinnan yhdistäminen varmenteiden hallintaan
- Kehitysprojektipalvelut
 - Erityistarpeiden asettamien kehitystarpeiden tunnistaminen ja ratkaisumäärittely
 - Uusien tarpeiden asettamien kehitystarpeiden tunnistaminen ja ratkaisumäärittely
 - Muutostarpeiden kehitysmäärittely ja roadmap-suunnittelun tukeminen

1.5. Palvelumallit

BBS:n PKI-palvelujen toimintakonsepti on hyvin joustava ja kustannustehokas. PKI-palvelut voidaan luoda ja tuottaa asiakkaalle kolmella eri vaihtoehtoisella tavalla: Managed PKI – varmennejärjestelmän hallintapalveluna, varmentajapalveluna tai asiakkaan itse toteuttaman PKI-järjestelmän hallintapalveluna.

Varmenteiden käyttöönottossa ja tilaus- ja hallintaprosessien toteuttamisessa Secure Link tarjoaa ammattitaitoisen kokonaispalvelun jonka ansiosta asiakasorganisaatio saa mahdollisimman suuren hyödyn varmenteista mahdollisimman pienellä vaivalla ja kustannuksilla.

Palvelujen väliset erot liittyvät varmennepalvelujen vastuun jakamiseen, eikä tekniseen tuotantoon. Kaikista palveluista syntyy SLA-sopimus, jossa määräytyy vastuut, toimitus- ja vasteajat, sekä kokonaishinta. Kokonaishinnalla varmistutaan siitä, ettei PKI-projektin hinta muutu tai aikataulu petä, eikä muutokset käyttäjämäärissä aiheuta ennakoimattomia kuluja. Yleensä voidaan sanoa, että käyttäjävarmenteiden sopimushaarukka liikkuu 50 tuhannen varmenteen välein. Näin asiakas säästyy yllätyksiltä ja turhilta pohdinnoilta yksittäisten lisenssien käytöstä, mikä helpottaa budjetointia ja kokonaiskustannusten hallittavuutta.

1.5.1. Managed PKI

Managed PKI -palvelumalli tarkoittaa sitä, että asiakas voi itse toimia varmentajana, joka julkaisee omat varmennepolitiikat, mutta hankkii varmennejärjestelmän täysin hallinnoituna kokonaispalveluna. Tällöin varmentaja luo SLA-sopimuksen siitä, kuinka paljon varmenteita tarvitaan, minkälaisia varmenteita tarvitaan (esim. laatuvarmenteet), mitä toiminnallisuuksia ja palveluja halutaan (WebRA-, mobiilivarmennepalvelut, validointipalvelut, jne.) ja mikä on käyttöaste millekin osiolle.

Managed PKI palvelu on hyvin joustava. Asiakas voi hyödyntää palvelua esimerkiksi nk. White Label – palveluna mikäli organisaatio haluaa myöntää varmenteita omille asiakkailleen tai kumppaneilleen kaupalliselta pohjalta. Koska lisäarvopalvelut kuten OCSP validointi on sidottu varmenteeseen, eivät erilaiset toimintamallit vaikuta palveluehtoihin tai hintaan. Palvelu mahdollistaa myös monien hyvin edistyneiden palvelujen käyttöönoton joiden avulla asiakasorganisaatio voi kehittää identiteetin hallintaa, käyttäjien roolipohjaista tunnistusta ja erilaisia valtuutuspalveluja sekä laitevarmennusta.

1.5.2. Varmentajapalvelu

Varmentajapalvelumalli tarkoittaa sitä, että BBS toimii varmentajana, jolloin asiakas ainoastaan mukauttaa BBS:n tarjoaman varmennepolitiikan omien tarpeiden mukaiseksi yhdessä Conseqs Oy:n asiantuntijoiden kanssa. BBS tarjoaa valmiit varmennekäytäntömääritykset ja varmenneympäristön halutun varmennepalvelutason mukaisesti (esim. laatuvarmennepalvelu). Varmennepalvelun SLA-sopimus kattaa mm. varmenteiden määrään, laatuun, voimassa oloon, vastuiden jakamiseen ja lisäarvopalvelujen käyttöön kuten OCSP validointipalveluihin liittyvät asiat.

Yksinkertaisimmillaan asiakas voi ostaa valmiita varmenteita BBS:n varmennepalvelusta ilman räätälöintiäkin. Varmenteet toimitetaan aina asiakkaan toivomalla tavalla, välineellä* ja profiililla. Kuten tiedettyä, varmentajien valmiit varmennetuotteet ovat erittäin kalliita ja monesti myös hyvin vaikeita ottaa käyttöön asiakasorganisaation normaaleihin käyttäjätunnisteiden hallintajärjestelmiin.

* Varmennevälineistä kuten toimikorteista, USB-avaimista, SIM tai Secure Memory –laitteista sekä näiden hallintapalveluista tulee pyytää erillistä tarjousta.

Mikäli asiakas tarvitsee erittäin korkealaatuisia laatu- tai edistyneitä varmenteita, jotka ovat laajasti tuettuja, hyväksytyjä ja yhteensopivia suurimassa osassa Eurooppaa, mutta ei tarvitse omaa PKI-järjestelmää, on BBS:n varmentajapalvelu sopivin vaihtoehto muille kaupallisille tai julkisille varmentajille.

1.5.3. Asiakkaan oman PKI-järjestelmän hallintapalvelu

Asiakas voi myös itse toteuttaa oman PKI-järjestelmän (esim. Microsoftin alustalle tai Open Source - pohjaisesti), jolloin asiakkaan oma PKI-järjestelmä voidaan siirtää BBS:n hallintaan. Asiakas saa tällöin käyttöönsä ISO 27001 -sertifioidun varmennepalveluympäristön ja hallinnan sekä kaikki mahdolliset muut palvelut, kuten kertakäyttösalasanapalvelut, SAML2 -tunnistuspalvelut, sähköisen allekirjoituksen workflow- ja arkistointipalvelut, tai vaikka mobiilivarmennepalvelut.

Itse toteutettu PKI tarjoaa toimivan vaihtoehdon silloin kun asiakas on itse räätälöinyt runsaasti omia erityisominaisuuksia ja palveluja, joita ei kannata tai voi siirtää toiselle alustalle. Tällaisessa tilanteessa BBS:n PKI-hallintopalvelu tarjoaa kustannustehokkaan ja nopean tavan mm. nostaa varmennejärjestelmän taso laatuvarmennetasoksi ja taata korkea varmuuden, käytettävyyden ja turvallisuuden taso omalle palvelulle. Kyseessä ei ole pelkkä hosting-palvelu, vaan asiakkaalle tarjotaan huolto- ja huolivapaa varmenneympäristöpalvelu ja kehitystä tukeva kokonaispalvelu. Luonnollisesti kaikki lisäarvopalvelut kuten OCSP validointi kuuluu pakettiin.

Kannattaa kuitenkin ottaa huomioon, että vaikka Microsoft tai Open Source PKI-järjestelmien lisenssikustannukset ovat olemattomat, ei BBS:n täysin hallinnoitu varmennejärjestelmäpalvelu välttämättä maksa yhtään enempää kuin oman PKI järjestelmän tuottaminen. Mikäli hinta on ainoa ratkaiseva tekijä, on BBS:n hallinnoima varmennepalvelu kokonaiskustannuksiltaan erittäin edullinen ratkaisu.

1.6. Tekninen tuki ja ylläpitopalvelut

Hallinnoidun PKI-palvelun osalta Secure Link Oy tuottaa kaikki määrittelyyn, pilotointiin, käyttöönottoon, tukeen, ylläpitoon, koulutukseen ja kehitykseen tarvittavat palvelut.

Tukitoiminta:

- BBS:n tuottamien PKI-palvelujen ensimmäisen tason paikallinen suomen ja ruotsinkielinen tuki
- 2 ja 3 tason tuen eskalointi BBS:lle 24/7 valmiudella

Ylläpitotoiminta:

- Käyttöhallinnan määrittely, dokumentointi ja koulutus
- Käyttöohjeistuksen suunnittelu ja toteutus yhdessä asiakkaan kanssa
- Eri asiakaspalvelutoimintojen määrittely, toteutus ja ylläpito
 - RA-rekisteröintipalvelujen tuottaminen, akkreditointi, valvonta, ylläpito ja tuki
 - RA-rekisteröintipisteen tai Web-liittymän tuottaminen, koulutus, ylläpito ja tuki

- Asiakasprojektien hallinta (määrittely, suunnittelu, kehitys, integraatiot, pilotointi ja käyttöönotto)
- Asiakassuhteiden hallinta (kaupalliset ja tekniset suhteet)

2. PKI-palvelun liittäminen ja hallinta

2.1. Varmenteiden hallinta

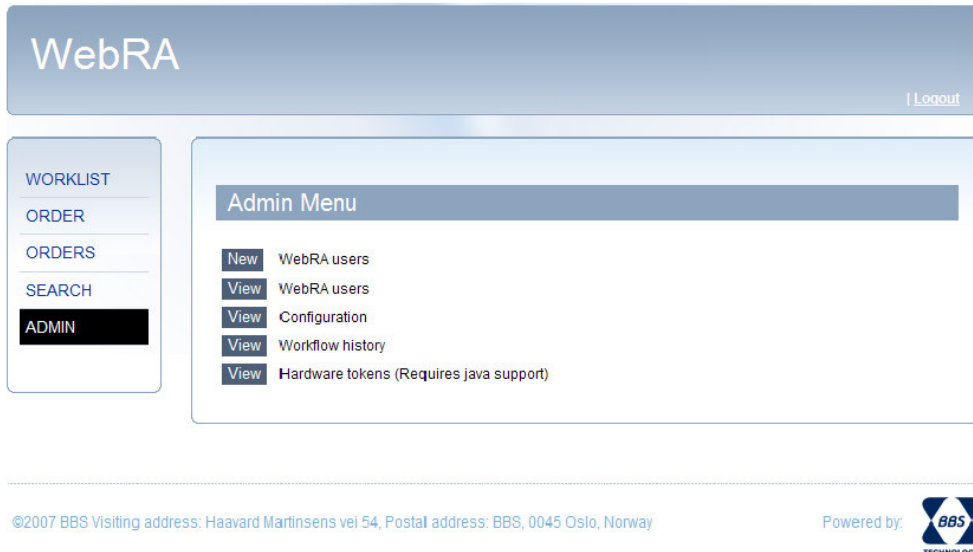
Hallinnoitu PKI-palvelu integroidaan osaksi asiakkaan omia hallintaprosesseja Request Management System (RMS) -välittäjäkomponentin avulla. RMS on käyttäjälle näkymätön "middleware" käyttöliittymä, jonka voidaan toteuttaa räätälöityjä rekisteröinti-, yksilöinti- ja hallintaratkaisuja ilman että taustalla olevasta PKI-järjestelmästä tarvitsee tietää mitään. Se voidaan myös liittää käytössä olevaan käyttäjähallintajärjestelmään, jolloin varmenteiden tilaus ja elinkaaren hallinta integroituu normaaliin käyttäjähallinnan prosessiin.

Request Management System on yksinkertainen API-rajapintasovellus, joka tarjoaa perinteistä PKI-järjestelmää laajemmat toiminnot ja toimii rajapintana PKI-palvelun ja asiakasjärjestelmän välillä. Asiakkaan ei tarvitse "sisäistää" PKI-järjestelmää, vaan palvelukokonaisuus toimii käyttäjille ja hallinnoijille läpinäkyvästi. Varmenteiden tilaus ja hallinta RMS järjestelmän avulla auttaa minimoimaan kaiken integraatiotarpeen asiakasorganisaation olemassa olevien tietojärjestelmien ja BBS:n hallinnoiman PKI-järjestelmän välillä. Varmenteiden hallinta tehdään standardeja XML-rajapintoja käyttäen siten että RMS API sovellus käsittelee kaikki toimintakutsut ja tietoturvaoperaatiot ilman että eri taustajärjestelmiin tarvitsee tehdä muutoksia.


Varmenteiden hallinta integroituu vaivattomasti kaikkiin identiteetin hallintajärjestelmiin, ainoa vaatimus on että IDM järjestelmä tukee Java-teknologiaa. Varmenteiden hallinta integroituu myös kaikkiin standardeihin PKCS#11 käyttöliittymärajapintaa hyödyntäviin sovelluksiin kuten HSM-laitteisiin ja toimikortteihin.

2.2. Varmenteiden hakeminen, julkaisu ja sulkeminen

RMS-järjestelmän ydintehtävä on toimia käyttöliittymänä varmenteiden hakemiselle, julkaisemiselle ja sulkemiselle PKI-järjestelmästä. Varmenteiden hakeminen (varmennepyyntö) on RA (Registration Authority) -valtuutetun toimijan vastuulla. RA-työpisteenä voi olla käytössä oleva käyttäjähakemistorekisterinpitäjän työpiste, joka pitää tosin vahvistaa käyttämään varmennekorttia käyttäjätunnistuksessa. Web RA-piste on myös mahdollinen samoin kuin erillinen RA-työasema.



©2007 BBS Visiting address: Haavard Martinsens vei 54, Postal address: BBS, 0045 Oslo, Norway

Powered by: 

Kuva 2: Varmenteiden hallinta WebRA-palvelun avulla.

Varmennepyynnöt voidaan automatisoida esim. identiteetin hallintajärjestelmään siten, että kun uusi käyttäjä rekisteröidään järjestelmään, tiedoista muodostetaan automaattisesti varmennepyyntö. Samoin kun käyttäjä poistetaan tai jos tila muutetaan, voidaan varmenteen sulkeminen tai uusinta automatisoida samaan prosessiin. Eri valmistajien identiteetin hallintajärjestelmät (SUN, CA, Oracle, IBM, Novell, Microsoft jne.) tarjoavat luonnollisen liittymän huomaamattomalle varmenteiden tilaamiselle ja sulkemiselle ilman, että asiakasorganisaation tarvitsee muuttaa toimivia käyttäjähallinnan prosesseja toisenlaisiksi PKI-palvelun takia.

Varmenteiden julkaisussa voidaan soveltaa useita eri toimintatapoja riippuen asiakkaan tarpeista. Perinteinen tapa on julkaista varmenteet joko julkiseen tai sisäiseen LDAP-hakemistoon ja lisätä suljetut varmenteet CRL-listalle. Tässä toimintatavassa on tärkeää, että käyttäjä tunnustetaan sekä varmenteen rekisteröinti- että myöntämisvaiheessa, koska varmenne on aktiivinen välittömästi kun se julkaistaan. Esimerkiksi PIN-PUK -kuoren katoaminen toimituksen aikana voi kasvattaa riskiä, että varmennetta on voitu käyttää väärin ja näin ollen turvallisuussyistä mm. HST-kortti annetaan haltijalle vain rekisteröijän toimesta.

Toinen tapa, joka tarjoaa parempaa joustoa sille missä tilanteessa varmenne otetaan varsinaisesti aktiivikäyttöön, on julkaista varmenne hakemistoon, mutta lisätä se samalla "Suspend" -tilaan CRL-sulkulistalle. Tämä luonnollisesti kasvattaa CRL-listan pituutta, mutta OCSP-validointipalvelua käytettäessä CRL-pituudesta ei ole haittaa. Tässä toimintamallissa käyttäjälle voidaan myöntää varmenne "kevyemmällä" prosessilla, koska varmenteen aktivointi voidaan tehdä myös muualla kuin rekisteröijän luona. Prosessi kevenee koska rekisteröijän ja aktivoinnin roolit voidaan eriyttää toisistaan, jolloin kummassakin vaiheessa voidaan toimia pienemmillä turvavaatimuksilla, edellyttäen tietenkin että prosessia noudatetaan oikein ja valvotaan asiallisesti. Aktivointi voidaan liittää mm. tilanteeseen, jossa kortinhaltijan kortille provisioidaan uusia palveluja. Olemassa olevien toimintatapojen hyödyntäminen vähentää merkittävästi varmennepalvelujen käyttöönoton hintaa ja tarvittavaa aikaa.

2.3. Valmis selaintuki omille varmenteille

Organisaatioiden itselleen myöntämät varmenteet eivät ole oletusarvoisesti luotettuja käyttäjien internet-selaimissa. Uusien Windows Vista –käyttöjärjestelmien osalta, myös luotettujen varmenteiden omatoiminen asentaminen selaimen on tehty entistä monivaiheisemmaksi. Tietoturvasyyt ovat ajaneet siihen, että selaimessa oletusarvoisesti luotettujen varmenteiden laatukriteerit on nostettu korkealle tasolle ja omien varmenteiden lisääminen on tehty käyttäjälle vähemmän helpoksi. Organisaation itselleen myöntämien varmenteiden käyttäminen selaimissa ilman häiritseviä varoitusilmoituksia tai omatoimisen asennuksen aiheuttamia lisäyövaiheita – joihin loppukäyttäjä pitää viimekädessä myös erikseen kouluttaa – on toteutettavissa kahdella tavalla. Ensimmäinen tapa on, että organisaation omat varmenteet allekirjoitetaan ennestään luotetun juurivarmentajan varmenteella. Tämä toimintamalli ei kuitenkaan ole joustavin mahdollinen koska juurivarmentajan politiikka ja sopimusehdot asettuvat organisaation omien politiikkojen ja ehtojen yläpuolelle. Toinen tapa on että asiakasorganisaation omat varmenteet esiasennetaan selaimiin selainvalmistajien toimesta. Tämä malli on toimivin organisaatiolle joka kaipaa mahdollisimman laajaa käytettävyyttä omille varmenteilleen.

Luotetun juurivarmenteen esiasennukselle on tiukat laatukriteerit ja vaatimukset, jotka BBS:n hallinnoima PKI-palvelu täyttää. Jotta varmenne voidaan esiasentaa selaimiin luotetuksi varmenteeksi, varmennepalvelun tuottajan on sertifioitava toimintansa ainakin yhden seuraavista standardeista mukaisesti:

- ETSI TS101 456
- ETSI TS 102 042
- WebTrust for Certificate Authorities

BBS:n hallinoidun PKI-palvelun ansiosta asiakasorganisaation on mahdollista täyttää yllälistattujen standardien vaatimukset ja saavuttaa tarvittava luotettavuustaso myös vaadittujen dokumentaation ja tietoturvaprosessien osalta.

3. Lisäarvopalvelut

3.1. Mobiilit tunnistuspalvelut

3.1.1. Kertakäyttösalasanapalvelu

BBS tarjoaa kertakäyttösalasanapalvelun (OTP – One-Time Password) mobiililaitteille sekä muille salasanalaitteille. Mobiilipalvelun ansiosta käyttäjä ei tarvitse muita välineitä kuin matkapuhelimensa vahvaa kahden muuttujan sähköistä tunnistusta varten. Samalle käyttäjälle voidaan antaa kertakäyttösalasanaratkaisu myös usealle eri välineelle, kuten toimikortille, USB-avaimelle tai muulle salasanalaitteelle. Mobiili ratkaisu tarjoaa helpon ja edullisen tavan tuottaa ja hallinnoida OTP-tunnistuspalvelu eri käyttäjille koska uusia tunnistusvälineitä ei tarvitse jakaa fyysisesti, eikä käyttäjien koulutus edellytä suurta ponnistusta.



Kertakäyttösalasanapalvelu mobiililaitteille perustuu Todos eCode Server teknologian ja Java MIDP mobiilipäätelaitesovellukseen. Käyttäjä voi ladata tarvittavan Java sovelluksen suoraan puhelimellaan jolloin OTP sovellus asennetaan puhelimeen. Sovelluksen turvataso vastaa finanssialan turvallisuusvaatimuksia ja helppokäyttöinen SMS-käyttöliittymä tarjoaa käyttäjälle helpon tavan tunnistautua turvallisesti eri verkkopaluihin. Todos eCode Server järjestelmään perustuvat kertakäyttösalasanapalvelut laajenevat helposti vahvan PKI-tunnistuksen ja sähköisten allekirjoitusten vaatimuksiin ja ratkaisu tarjoaa markkinoiden joustavimman ja monipuolisimman segmentoivan turvallisuusarkkitehtuurin OTP-tunnistukseen.

3.1.2. Wireless PKI -palvelu

Mobiilivarmennot ja mobiilivarmennepalvelujen tuottaminen on yksi BBS:n hallinnoitun PKI:n tarjoamia palveluja. Palveluun kuuluu koko mobiilivarmenne ”ekosysteemin” toteuttaminen, hallinta ja ylläpito asiakkaan tarpeisiin. Palvelun pääasiallinen asiakaskohde ovat teleoperaattorit, mutta BBS tarjoaa myös käyttäjään ratkaisut valmiina palveluna, jolloin organisaatio voi helposti ja edullisesti tarjota palveluja käyttäen mobiilivarmennot käyttäjätunnistukseen, tunnistuksen federointiin, kertakirjautumiseen, sähköiseen allekirjoittamiseen sekä käyttäjien provisiointiin.

Varmennepalvelun joustavuuden ansiosta asiakkaan on helppoa ja edullista laajentaa myös olemassa olevaa palvelusopimustaan kattamaan esim. mobiilivarmennepalvelut. Palveluntarjoajat voivat edullisesti ja vaivattomasti tarjota asiakkailleen suojattuja verkkopalveluja ja niihin tunnistus- sekä sähköisen allekirjoituksen palvelut käyttäen mobiilivarmennot. BBS:n palvelu perustuu ETSI standardin mukaiseen Wireless PKI alustaan (Valimo Wireless).

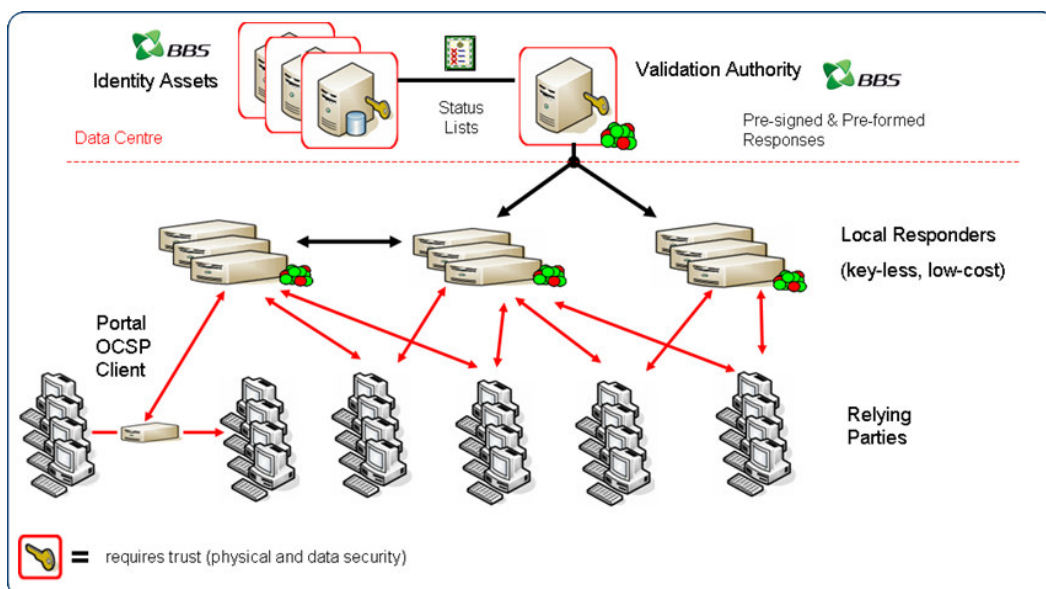
3.2. Varmenteiden validointipalvelut

3.2.1. Korkean käytettävyyden Validation Authority -validointipalvelu

Varmennevalidointi kertoo onko käyttäjä oikeutettu käyttämään palveluja tai resursseja ja niinpä luottosuhteiden hallinnassa validoinnin käytettävyys on olennaisen tärkeää. Varmenteiden validointi on vahvan tunnistuksen keskeinen haaste: suuret, hajautetut ja heterogeeniset organisaatiot törmäävät luottosuhteiden hallinnan ja validoinnin konkreettisiin haasteisiin päivittäin. Sulkulistojen hallinta on työlästä ja syö paljon verkkoresursseja, sulkulistojen käytettävyys on heikkoa koska päivitys edellyttää aina verkkoyhteyttä ja listat vanhenevat usein ennen kuin käyttäjä ehtii kahden kirjautumisen välissä päivittää niitä. Käytettäessä vanhentuneita sulkulistoja, organisaatiot altistuvat useille ongelmille, kuten:

- Käyttäjätietojen status on saattanut muuttua
- Vanhentunut sulkulista siirtää laillisen ja taloudellisen vastuun mahdollisista väärinkäytöksistä suoraan käyttäjälle
- Skaalautuvuusongelmat hidastuttavat verkkopalveluihin kirjautumista, mikä omalta osaltaan heikentää palvelujen käytettävyyttä
- Huonosti toimiva varmenteiden tarkistus heikentää PKI-palvelun investoinnin arvoa koska tietoturva ja luottamus eivät ole sillä tasolla mistä asiakas on maksanut

Perinteisiin CRL-sulkulistoihin, uudempiin Delta-CRL -listoihin ja perinteisiin OCSP Responder -palveluihin verrattuna hallinnoitu korkean käytettävyyden hajautettu Validation Authority -palvelu tarjoaa hyvin monipuolisen sovellettavuuden ja toiminnan vapauden.



Kuva 3: hallinnoitu varmenteiden validointipalvelu. BBS ylläpitää validointijärjestelmää, johon liitetään eri varmentajien sulkulistat. Paikallisella tasolla ainoastaan jaellaan ajantasaiset sulkutiedot käyttäen OCSP (Online Certificate Status Protocol) -tekniikkaa. Validointipalvelu mahdollistaa tavallista OCSP:tä monipuolisemmat toiminnot, kuten aika- ja paikka- tai sääntösidonnaiset lisäattribuutit tai estot.

Validointipalvelujen ansiosta hallinnoitua PKI-palvelua käyttävä organisaatio voi hyödyntää varmenteita missä tahansa toisessa organisaatiossa. Validoinnin piiriin voidaan tuoda muiden varmentajien sulkulistat, jolloin luottosuhteet eri varmentajien varmenteisiin voidaan hallinnoida keskitetysti koko maan alueella tai jopa eri maiden välillä. Kansainvälisen opiskelija- ja tutkijavaihdon, sekä erilaisten organisaatorajat ylittävien hankkeiden käyttäjähallinnassa voidaan hyödyntää omaa PKI-palvelua koska varmenteiden validointi mahdollistaa varmentaja-tason luottosuhteiden toimivan hallinnan. Käyttäjätason luottosuhteiden hallintaa voidaan kehittää identiteettien federaation kautta jos käyttäjävarmenteen luotettavuus voidaan tarkastaa ja taata.

3.2.2. Global Validation Service allekirjoitusvarmenteiden validointiin

BBS:n tarjoaman Global Validation Service GVS palvelun ansiosta sähköisesti allekirjoitetut asiakirjat ja varmenteet voidaan hyväksyä yli organisaatio- ja maarajojen, ilman että osapuolet ovat ennestään asioineet keskenään ja ilman, että osapuolilla olisi ennalta solmittuja varmennepalvelujen luottosuhteita. GVS-palvelu suorittaa allekirjoitusvarmenteiden tarkistuksen ja validoinnin ja antaa takeen validoinnin tuloksesta, eikä asiakirjoja keskenään vaihtavien organisaatioiden tarvitse itse luoda varmenteiden hyväksyttämiskäytäntöjä tai -sopimuksia, jotka ovat hyvin työläitä ja käytännössä hyvin ongelmallisia.

BBS toimii puolueettomana varmenteiden validoijana jolloin eri varmennepalvelun käyttäjät voivat hyödyntää sähköisiä palveluja ilman, että allekirjoitusten yhteensopivuudesta tai lainvoimaisuudesta tarvitsee itse kantaa huolta. Palvelun ansiosta varmenteiden hyödyntäminen on mahdollistaa organisaatio- ja valtiorajat ylittävästi. Sähköisen laskutuksen, kaupankäynnin, sopimusverkostojen luonnin ja finanssipalveluiden rajat ylittävyys voidaan toteuttaa luotettavasti, koska:

- Palvelu mahdollistaa usean varmentajan ja allekirjoitusteknologian luotettavan ja yhtenäisen käsittelyn, eli vähentää varmenteiden hyväksymiseen liittyvää teknistä ja hallinnollista monimutkaisuutta
- palvelu tuo yhteensopivuuden eri varmennepalvelujen myöntämien varmenteiden sekä eri sähköisten allekirjoitustekniikoiden ja -formaattien välillä
- palvelu antaa Det Norske Veritasin (DNV) julkisesti vahvistetun laatukriteerien mukaisen riskiarviointiin perustuvan laatu- ja turvallisuusluokituksen kullekin varmenteelle, sähköiselle allekirjoitukselle ja varmentajalle, antaen täten tehokkaat keinot hallita rajat ylittävien sähköisten asiointiprosessien ja palvelujen laillisia ja taloudellisia riskejä

Validointipalvelu toimii seuraavalla tavalla:

Global Validation Service validointipalvelu solmitaan varmenteita myöntävien julkisten ja kaupallisten varmennepalvelutarjoajien kanssa. BBS luo varmentajien kanssa yhteisen ansaintamallin sekä toimintamallin organisaatio- ja maarajat ylittävien yhteensopivien sähköisten allekirjoitusten hyödyntämiselle. Eri toimijoiden roolit ja tehtävät jakautuvat seuraavasti:

- **Varmennepalvelut:**

Lain voimaisia laatuvarmenteeseen perustuvia allekirjoitusvarmenteita myöntävät varmentejat ja sähköisten henkilövarmenteiden myöntäjät.

- **Allekirjoittajat:**

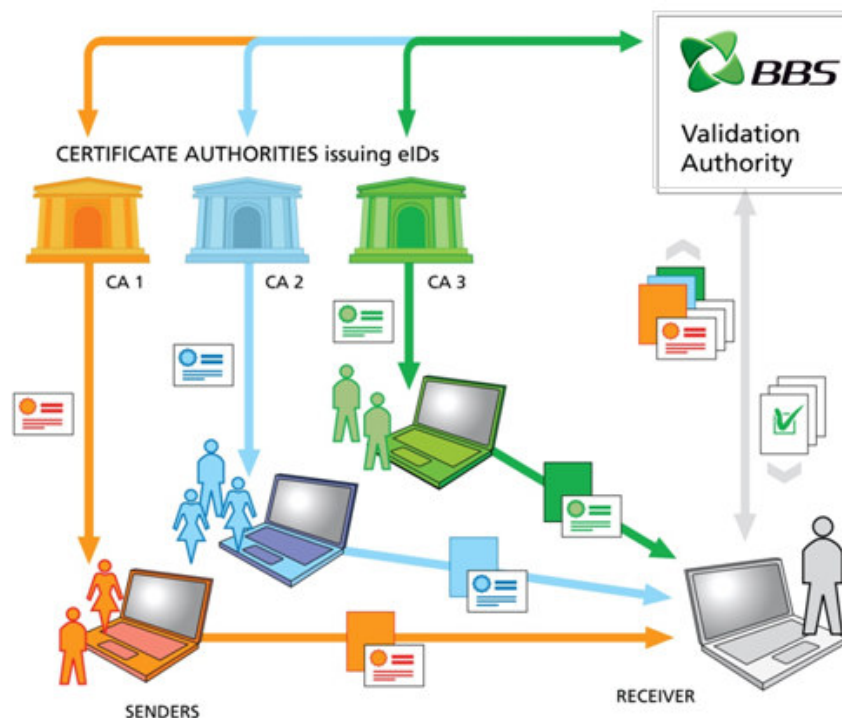
Varmenteiden käyttö allekirjoittamisessa: käyttäjä allekirjoittaa asiakirjan lain voimaisella laatuvarmenteeseen perustuvalla sähköisellä allekirjoituksella

- **Allekirjoitusten tarkistaja:**

Antaa allekirjoitetun asiakirjan varmenteen tarkistettavaksi BBS:n GVS-palvelulle. BBS suorittaa allekirjoituksen tarkistuksen, validoi allekirjoitusvarmenteen voimassaolon ja arvioi, sekä vahvistaa allekirjoituksen lain voimaisuuden, laadun tai valtuuden.

- **Allekirjoituksen vastaanottaja:**

Vastaanottaa allekirjoitetun asiakirjan ja saa BBS:n GVS-palvelulta vahvistuksen allekirjoituksen voimassaolosta, lain voimaisuuden, laadusta tai allekirjoittajan valtuuksista.



Kuva 4: GVS palvelun osatekijät: usea varmentaja ja useita varmenteiden käyttäjiä. Luottamusta kaikkiin eri varmenteisiin on mahdoton hallita ellei käytössä ole yhtenäistä viitekehystä minkä kautta luottamus määritellään, sekä palvelua joka tarjoaa luotettavuuden arvioinnin automatisoidusti. BBS:n palvelu on tässä suhteessa ainutlaatuinen koko maailmassa.

4. Hallinnoitu PKI-palvelu vertailussa

Varmennetietojärjestelmien valikoima on hyvin runsas, mutta tiettyjä suuria tendenssejä ja vaihtoehtoja voidaan kuitenkin tunnistaa. Erilaiset COTS ratkaisut (Commercial Off The Shelf), joiden tavalla asiakas voi itse luoda oman varmennepalvelun hallitsevat kansainvälisiä PKI-markkinoita, mutta uusia palvelumalleja on kehitetty rinnalla, missä teknologinen High-End ja korkean turvatason palvelutarjonta yhdistyvät toimiviksi kokonaispalveluiksi. BBS on pohjoismaiden suurin varmentaja ja samalla yksi Euroopan suurimmista hallinnoitujen PKI-palvelujen tuottajista, jolla on kokemusta PKI-järjestelmien tuottamisesta, hallinnasta ja vaativasta palvelutuotannosta yli kymmenen vuoden ajalta. Vertailemme tässä kappaleessa tyypillisiä PKI-järjestelmiä ja toteutusmalleja BBS:n tarjoaman palvelun suhteen. Vertailu ei pyri osoittamaan tietyn ratkaisun paremmuutta toisesta vaan nostamaan esille ne kysymykset ja asiat, jotka ovat merkitseviä silloin kun asiakas arvioi objektiivisesti PKI-järjestelmän hankkimista palveluna tai itse tuotettavana ratkaisuna.

4.1. Valmiit PKI-järjestelmät ja -ratkaisut

4.1.1. Suuret kaupalliset PKI-järjestelmät

Suuret kaupalliset PKI-järjestelmät kuten mm. Entrust, RSA, Cybertrust, joiden käyttöön myös BBS:n PKI-palvelu perustuu, on suunnattu lähinnä sellaisille organisaatioille, joille oman varmennepalvelujärjestelmän toteuttaminen, ylläpito ja kehittäminen kuuluvat liiketoiminnan ydintoimintaan.

Monet suuret kansainväliset yritykset ovat niin suuria, että organisaation sisäiset asiakkaat muodostavat jo omat varmennemarkkinansa, joille itse tuotetut palvelut voidaan tarjota kaupallisesti järkevällä tavalla. Lisäksi moni suuri organisaatio saattaa haluta toteuttaa itse oman PKI-palvelunsa kaupallisten järjestelmien avulla puhtaasti strategisista syistä, jolloin investointikustannuksia tai resurssien käyttöä arvioidaan muusta kuin puhtaasti taloudellisesta ja hallinnollisesta näkökulmasta. Tällaisia organisaatioita ovat yleensä valtiolliset toimijat tai suuryritykset joiden liiketoiminta-ala on erityisen tietoturvakriittistä, kuten esim. tai puolustusteknologia- tai finanssiala.

Kuvaavaa näille kahdelle asiakasryhmälle on kuitenkin se, että kummallakin on sekä taloudelliset resurssit, että strategiset ohjelmat joiden avulla organisaatiot voivat toteuttaa PKI-palvelun juuri niin korkealle turvallisuuden ja luotettavuuden tasolle kuin mitä teknologialla ja prosesseilla pystytään. Tässä asemassa ei kuitenkaan ole kuin häviävän pieni osa yrityksistä – edes suurista sellaisista. Jopa valtiollisella tasolla, mm. USA:ssa PKI-järjestelmät toteutetaan systemaattisesti palveluhankintana luotettavilta palveluntarjoajilta. Suomessa tämän toimintamallin omaksuminen on vielä uutta, mutta kun tarkastelee usean eri PKI-hankkeen elinkaaren kustannuksia ja muita haasteita jotka ovat kohdanneet niitä ajan saatossa, voidaan objektiivisesti todeta, että ehkä valitut toteutusmallit eivät ole olleet kaikista kustannustehokkaimmat.

BBS:n tarjoama hallinnoitu PKI-palvelu tarjoaa edullisimman tavan ottaa käyttöön korkean tason PKI-järjestelmä omaan käyttöön: edullisimmillaan täysin hallinnoitu palvelu voi maksaa saman verran kuin pelkkä PKI-alustan lisenssi!

4.1.2. Pienet kaupalliset ja Open Source järjestelmät

Pienempien kaupallisten ja Open Source PKI-järjestelmien suhteen moni organisaatio pyrkii arvioimaan tarjotun teknologian säilyvyyttä niin lähdekoodin kuin kehitys- ja ylläpitoressurssien osalta.

Poislukien korkeakoulut, joilla on itsellään mahdollisuus kehittää ja ylläpitää Open Source PKI-järjestelmiä ilman kohtuuttomia taloudellisia riskejä, organisaatioilla ei yleensä ole mahdollisuutta sijoittaa PKI-järjestelmän resursseihin niin suurta tieto-taitopääomaa, jolla Open Source ratkaisun ylläpito voitaisiin turvata pitkäksi ajaksi. Palveluna tuotettuna Open Source teknologia voi olla toimiva ratkaisu edellyttäen että itse palveluntarjoaja voi taata pysyvyyden ja jatkuvuuden. Tämä ei kuitenkaan yksin takaa sitä, että PKI-palvelu olisi erityisen edullinen asiakkaalle: koska ammattitaitoinen henkilöstö on yksi PKI-palvelun suurimmista kustannuseristä, voi yhtenä esimerkkinä pitää sitä, että BBS voitti Baltian maassa mobiilivarmennepalveluista tehdyn laatuvarmennekilpailutuksen Viron SK:ta vastaan. BBS:n mobiili laatuvarmennepalvelu oli 30% edullisempi kuin SK:n vastaava, vaikka SK:n palvelu on tuotettu Open Source -pohjaisesti, pelkkien henkilöstökustannusten ajaessa palveluhintaa.

Koska monen Open Source –tarjoajan PKI-ratkaisu perustuu ei-kaupalliseen puhtaasti palvelupohjaiseen liiketoimintamalliin, voi moni asiakasorganisaatio pitää tätä toimintatapaa riskialttiina muutoksille IT-markkinoilla, yhteiskunnassa tai keskeisten kehittäjien ja ylläpitäjien henkilökohtaisessa elämässä. Samanlaiset huolet voivat vaikuttaa myös siihen ottaako asiakasorganisaatio käyttöönsä pienen itsenäisen toimittajan kehittämän PKI-alustan.

Päin vastoin kuin Open Source –alustoilla, ei kaupallisilla alustoilla ole laajaa kehittäjäkuntaa ja usein pienissä PKI-kehitysyhteisöissä kaikki kehitystyö tehdään pienissä tiimeissä joilla saattaa olla hyvin suuri tarve pitää PKI-tuote mahdollisimman pelkistettynä, jotta ylläpidettävän kokonaisuuden laajuus ei kävisi ylivoimaiseksi hallita pienellä tiimillä. Pienen ja pelkistetyn PKI-alustan edut ovat lukuisat erityisesti silloin kun haetaan sovellus- tai käyttökohtaisia ratkaisuja, mutta monesti pelkistys rajoittaa järjestelmän käyttömahdollisuuksia useisiin eri tarpeisiin. Tämä voi johtaa siihen että asiakasorganisaatio voi joutua joko itse rahoittamaan erilaisten laajennusten kehitystä erillisinä kehitysprojekteina tai ottamaan käyttöön rinnalle toisen PKI-järjestelmän.

Kummassakin tapauksessa kustannusten hallinta on erittäin haasteellista ja syntyvän PKI-legacyyn paino saattaa tulla vastaan tulevaisuudessa mikäli varmenteiden käyttöä pitää laajentaa ja kasvattaa. Lisäksi koska kaupallisen PKI-alustan lähdekoodi ei ole avoin, saattaa alustan ylläpito olla hyvin vaikeaa jos teknologian kehittäjä lopettaa toimintansa syystä tai toisesta. Myöskään nk. Escrow sopimukset eivät välttämättä korjaa tällaisesta riskistä syntyneitä vahinkoja koska kehittäjäresurssit saattavat olla hyvin vaikeasti hankittavissa jos PKI-alustan käyttäjäkunta on ollut suppea, eikä kyseisen teknologian ympärille ole syntynyt laajaa käyttäjäyhteisöä.

4.2. Microsoft Windows Server varmennepalvelut

Microsoft Windows Server ympäristö tarjoaa varmennepalvelut, eli nk. Certificate Authority (CA) toiminnot osana Windows-palvelimen lisenssiä. Kyseessä on luotettava ja helposti käyttöön otettava tietoturva-järjestelmä jolla organisaatio voi kehittää ja ylläpitää sisäisiä tietoturvallisia prosesseja, käyttäjätunnistusta ja salata arkaluontoisia tietoja PKI-pohjaisesti. Organisaation sisäisten prosessien

suoraviivaiseen suojaamiseen Microsoft CA tarjoaa erinomaisen ratkaisun, joka on helppo laittaa käyntiin ja edullinen käyttää kun uusia lisenssejä ei juuri tarvitse ostaa.

Verrattuna BBS:n tarjoamaan hallinnoituun PKI-palveluun, Microsoft CA-järjestelmässä on kuitenkin rajoitteita, jotka on tärkeä ottaa huomioon silloin kun valitaan organisaation tarpeisiin parhaiten sopivaa PKI-järjestelmää. Tässä muutama merkitsevä eroavaisuus, jotka tulee ymmärtää valintaa tehtäessä:

- BBS:n hallinnoitu PKI-palvelu tarjoaa erittäin kattavan tuen auditoinnille, lokien pidolle ja vastuiden sekä roolien erottamiselle (Segregation of Duties / SoD), mihin Microsoft CA-järjestelmässä on selkeitä rajoitteita, jotka voivat vaikuttaa siihen miten sillä tuotettua PKI-palvelua voidaan kehittää palvelemaan muuttuvia tarpeita ja vaatimuksia
- Omien varmennelaajennusten (Certificate Extensions) käyttäminen henkilö- ja laitevarmenteiden kanssa tukee varmennepohjaisia roolimäärityksiä, käyttöoikeuksia ja erilaisia käyttö- tai pääsyvaltuutuksia. Microsoft CA-järjestelmässä varmennelaajennukset ja asiakaskohtaiset räätälöinnit ovat hyvin rajoittuneesti tuetut tai niiden käytöstä aiheutuu paljon ongelmia. BBS:n hallinnoitu PKI-palvelu tarjoaa laajan tuen erilaisille X.509v3 varmennestandardin mukaisille laajennuksille ja asiakaskohtaisille räätälöinnille, mikä takaa laaja-alaisen käytettävyyden PKI-palvelulle myös hyvin pitkällä ajalla
- Varmenteiden rekisteröinnissä nk. Registration Authority (RA) toiminnot tuotetaan Microsoft Active Directoryn avulla, mistä seuraa se, että ne oikeutetut käyttäjät jotka voivat hallinnoida Windows AD hakemistopalveluja saavat automaattisesti pääsyn myös itse RA tietokantaan. Tämä on haaste tietoturvan hallinnalle mikäli organisaatiolla on tarve ylläpitää tiettyjen standardien mukaisia tietoturvaprosesseja, kuten esimerkiksi PCI-DSS:n asettamia vaatimuksia.
- BBS:n hallinnoitulla PKI-palvelulla vältetään RA-tietokantaan pääsy asiattomilta, hallinnoidaan varmenteiden salaiset avaimet ja arkistoidaan salausavaimet ilman rajoitteita jotka saattavat johtua Windows AD:n ominaisuuksista. Koska Windows palvelin ei ole yksistään varmennetietojärjestelmä, on luonnollista että PKI-toiminnalle erityisiä ominaisuuksia on toteutettu osittain kompromissina muiden AD-toimintojen ja palvelujen kanssa.
- Kun asiakasorganisaatio perustaa PKI-palvelunsa BBS:n hallinnoitulle palvelulle, voidaan yleisiin tietoturvariskeihin ja haasteisiin vastata Windows palvelintasolla ilman, että organisaation luottamusverkoston ytimenä toimivaan varmennepalveluun tarvitsee kajota, tai sen luotettavuutta vaarantaa. Palveluiden segmentoiminen tällä tasolla on selkeä valtti kun organisaation tietoturva- ja haavoittuvuusriskejä arvioidaan objektiivisesti.

4.3. Mitä PKI maksaa itse toteutettuna palveluna?

4.3.1. Varmennepalvelujärjestelmän kertakustannuslaskelma

Alla olevassa taulukossa on listattu tavanomaiset kertakustannukset PKI-järjestelmän toteuttamisesta kolmen vuoden sopimusajalle.

HUOM! Kustannuksissa on laskettu vain PKI-järjestelmän hallintaan ja tekniseen toteuttamiseen liittyvät kustannukset, Ei varmennetietojärjestelmän (PKI) mahdollista lisenssikustannusta, Ei tarvittavan Enterprise-tason tietokantaohjelmiston hintaa, eikä muita mahdollisia lisenssikustannuksia PKI-sovelluksista, tilaus- ja hallintalisäosista, OCSP-validointijärjestelmästä tai esimerkiksi LDAP-hakemistoista. Näiden kokonaiskustannukset voivat nousta aina 500 000 euroon asti, tai yli. Kustannuslaskelma olettaa että

asiakasorganisaatio käyttää jo olemassa olevia lisenssejä tai PKI-järjestelmää, josta ei ole lisenssikustannuksia (Microsoft CA tai Open Source tuote).

	Itse tuotettu
Suunnittelu ja arvioiminen	120 000
Turvalliset tilat	40 000
Laitteistot ja sovellukset	85 000
Asennukset ja määrittelyt	60 000
Varautumisjärjestelyt	95 000
Varmuuskopiointi	10 000
Juuriavaimen luonti ja kokonaiseremonia	80 000
Auditointi	50 000
Ylläpito ja operatiivinen hallinta	20 000
Loppukustannukset	564 000

Laskelman perustelut:

- Suunnittelu ja arvioiminen: 4 henkilöä, 3 kuukautta à 500 euroa / päivä
- Turvalliset tilat: muutostyöt, testaus, rakentaminen, hyväksytys
- Laitteistot ja sovellukset: palvelimet, HSM laite, verkkoelementit, hallintasovellukset
- Asennukset ja määrittelyt ja testaus: 2 henkilöä, 15 päivää à 500 euroa /päivä
- Varautumisjärjestelyt: kahdennetut palvelimet, HSM laitteet, verkot, lisenssit, kahdennettu sijoituspaikka, testaus
- Varmuuskopiointi: avainten varmuuskopiointi, salausavainten palautus, CA-avainten varmuuskopiointi ja hallintamenettelyt
- Juuriavaimen luonti ja kokonaiseremonia: Root Key Generation (RKG) seremonian suorittaminen, jossa seremoniamenettely, auditoinnin todistus, RKG testaus ja harjoitustilaisuudet
- Auditointi: varmennepolitiikkojen ja -käytäntöjen (CP ja CPS) noudattamisen seuranta, tietoturvastandardien mukaisen toiminnan tarkastaminen, laatuvarmistuksen mukaisen toiminnan tarkastaminen ulkopuolisen puolueettoman auditoinnin toimesta. Auditointi viitekehysten luominen.

- Ylläpito ja operatiivinen hallinta: ylläpidon ja operatiivisen hallinnan prosessien luominen 99,5% – 99,7% käytettävyyssasteen ja 24h valvonnan vaatimustasolle, 2 henkilöä, 20 päivää à 500 euroa / päivä

4.3.2. Varmennepalvelujärjestelmän vuosittaisten kustannukset

Alla olevassa taulukossa on listattu tavanomaiset vuosittaiskustannukset PKI-järjestelmän ylläpidosta kolmen vuoden sopimusajalle.

	Itse tuotettu
Suunnittelu ja arvioiminen	0
Turvalliset tilat	15 000
Laitteistot ja sovellukset	15 000
Asennukset ja määrittelyt	0
Varautumisjärjestelyt	9 000
Varmuuskopiointi	10 000
Juuriavaimen luonti ja kokonaiseremontti	0
Auditointi	50 000
Ylläpito ja operatiivinen hallinta	150 000
Loppukustannukset	249 000

BBS:n PKI-palveluiden kustannukset ovat perustamiskustannusten osalta 30% – 50% alhaisemmat kuin itse tuotetun PKI-järjestelmän. Vuosittaisten kustannusten osalta BBS:n palvelu on 20% – 30% alhaisemmat kuin itse tuotetun palvelun. Tarkemman BBS:n palveluhintojen vertailun saa Secure Link Oy:n kaupalliselta edustajalta.

5. PKI-projekti

5.1. Yleiskatsaus

BBS:n tuottama hallinnoitu PKI-palvelu on tehokkain tapa toteuttaa korkean käytettävyyden ja turvallisuustason PKI-palvelut. Hallinnoituun PKI-projektiin kuuluu määritysten suunnittelu, palvelusopimuksen laatiminen, testaus ja pilotointi, sekä käyttöönotto. PKI-projekti jaetaan osaluokkiin, jotka on esitelty alla olevissa kappaleissa.

5.2. Määrittelyt

5.2.1. Tekniset määrittelyt

Teknisellä määrittelyllä tarkoitetaan PKI-tekniikkaan liittyvien tekijöiden määrittelyä. Tämä sisältää seuraavat asiat:

- Varmennepolitiikat
- Varmenneprofiilit
- Varmenteiden käyttötarkoitukset (eri varmennetyypit henkilö- tai laitevarmenteille)
- Varmennehierarkia ja CA-tasot (yhden tai useamman Sub-CA tason hierarkiat)
- Eri varmennealustat (sovellus, TPM-siru, toimikortti, SIM-kortti, USB, kertakäyttösalasana-laite)
- Mahdollisen toimikortin varmenne-sovellus (voi olla myös USB-avain tai muu turvallinen väline)
- Varmenne-sovelluksen profiili (jos varmenne on sirulla)
- Varmennekorttikäyttöliittymän vaatimukset ja toiminnot
- Kertakäyttösalasana-ratkaisun määrittely

Teknisissä määrittelyissä ratkaistaan myös varmenne-palvelutyyppi:

- Managed PKI palvelu (myös nk. White Label PKI)
- BBS:n varmenne-palvelu
- Itse toteutetun PKI-järjestelmän ylläpitopalvelu

Lisäksi määritellään palvelutyypistä riippuen seuraavat asiat:

- Request Management System –integraatio (HR, LDAP, muu)
- Integraatorajapinnat varmenteiden hallinnalle
- RMS-toiminnallisuus ja WebRA –palvelun luominen
- Oman PKI-palvelun osalta tehdään erillinen projektisuunnitelma ja toimintaehdotus

5.2.2. SLA-sopimuksen määrittely

BBS:n tarjoama hallinnoitu PKI-palvelu perustuu yhteen kokonaiseen Service Level Agreement (SLA) -sopimukseen. Sopimuksessa sovitaan mm. seuraavista perusasioista:

- PKI-palvelun tyyppi
- Hierarkia ja profiilityypit
- Palvelun kesto (24, 36, 48, 60, 72 kk)
- Varmenteiden määrä (50, 100, 300, 500 tuhatta, enemmän)
- Varmenteiden ja prosessin turvataso (Advanced, Qualified)
- Vasteajat ja käytettävyys / saatavuustaso (99,5% - 99,7%)
- Varmennemediat: token-varmenteet, mobiilivarmenteet
- Validointipalvelut ja niiden palvelutaso (OCSP ja Extended OCSP)
- Asiakkaan yhteyshenkilön koulutus ja osaamistasosta huolehtiminen

5.3. *Pilotointi, testaus ja käyttöönotto*

Hallinnoidun PKI-palveluin pilotoiminen voidaan toteuttaa hyvin nopealla aikataululla koska pilotoinnin voi aloittaa esimerkiksi pelkillä varmenteilla ilman integraatio- tai lisäpalvelutarpeita. Pilotoinnin suunnittelussa käydään asiakkaan kanssa läpi pilotoinnin sekä lopputilanteen tavoitteet, päämäärät, laajuus ja kesto, sekä luonnollisesti budjetti.

Testauksesta vastaa PKI-ydinjärjestelmän osalta BBS yksin, muilta osin asennettujen järjestelmien, ohjelistojen ja laitteiden testaus suunnitellaan ja toteutetaan yhdessä asiakkaan kanssa siten, että toimittaja vastaa dokumentaatiosta ja muutostöistä.

Käyttöönotto teknisenä toimenpiteenä voi olla tilanteesta riippuen hyvin nopea vaihe. Useissa organisaatio-PKI -hankkeissa käyttöönotto on kestänyt enimmillään kolme kuukautta. Varmennepalveluhankkeen tekninen käyttöönotto on kuitenkin aina nopeampi kuin määrittely- ja toimintaprosessien suunnittelu- ja toteutusvaiheet.

5.4. *Seuranta ja palvelujen kehittämien*

Hallinnoidun PKI-palvelun seuranta tapahtuu SLA-sopimuksessa määritellyin ehdoin.

Palvelujen kehittämisen osalta tarjoamamme palvelu mahdollistaa erittäin monipuoliset kehitysnäkymät ja -polut. Olemassa olevien asiakas-, käyttäjä- ja muiden palvelujen ja -prosessien kehittäminen onnistuu helpommin kun merkittävä osa tietoturvallista kokonaisarkkitehtuuria on tehokkaasti hallinnassa, eikä asiakkaan resurssit kiinnity PKI-hallintaan.

Tulevien kehitystarpeiden identifiointien lisäksi palveluja voidaan myös kehittää ennakoivasti ja suuntaa näyttävästi. Varmennepalveluiden tuottaminen asiakastarpeiden mukaisena ulkoistettuna palveluna siten, että palvelu skaalautuu globaalille tasolle ilman lisäponnisteluja tarjoaa asiakkaalle poikkeukselliset mahdollisuudet kehittää liiketoimintaa avoimilla markkinoilla internetissä ja muita kanavia hyödyntäen. BBS:n ja Secure Link Oy:n tuottamaa hallinnoitua PKI -palvelua vastaavaa toimivaa kokonaisuutta ei toistaiseksi Suomessa ole ollut tarjolla.

Lisätietoja ja yhteystiedot

Lisätietoja hallinnoidusta PKI –palvelusta antaa Secure Link Oy:n Teemu Rissanen.

Puhelin: 020 - 798 1340

GSM: 050 - 379 53 43

Sähköposti: teemu.rissanen@securelink.fi

Web: www.securelink.fi

Secure Link Oy

Hämeentie 153 B
00560 HELSINKI
Finland

TEL: +358 (0)20 798 1340
E-mail: sales@securelink.fi

URL: www.securelink.fi
VAT: FI14800922