



KATEVARMENNUS TCP/IP - YHTEYDELLÄ

**Versio 2.3
27.11.2008**



KATEVARMENNUS TCP/IP - YHTEYDELLÄ

Muutosluettelo

<u>Versio</u>	<u>Sivu</u>	<u>Muutos</u>
V2.1	Kaikki	Muutettu vastaamaan CA-palvelun mukaista toteutusta
V2.2	6 – 7	Lisätty vpn-client parametrit-tiedot
		Muutettu IPSec-parametrien arvoja
	10	Lisätty ip-osoitetieto varmenteeseen
	11	Poistettu varmenteen tietosisältöä kuvaava taulukko
	Liite 1	Poistettu vanhentuneella varmenteella tehtävät testit
	Liite 2 ja 3	Liitteet yhdistetty ja poistettu pre-shared keyn käyttö
	Liite 3	Uusi liite lisätty
V2.3	Kaikki	Suomen Pankkiyhdistyksen tilalle Finanssialan Keskusliitto ja dokumentti-tunnus vaihdettu CA05001:ksi (oli MPJ 05001)
	10	Muotoiltu laitevarmenteen yksilöivien tietojen esittämiskohtaa

Hyväksyntä

Version _____ pvm _____ Hyväksyjä

**KATEVARMENNUS TCP/IP - YHTEYDELLÄ****Sisältö**

1 JOHDANTO	4
2 SIIRTO-OTSAKE	5
3 TCP/IP YHTEYDET	6
3.1 Asiakkaan vpn-yhteys	6
3.2 Sulkulistan tarkastus	6
3.3 IPSec-yhteysparametrit	6
3.3.1 VPN-gateway	6
3.3.2 VPN-client	7
3.4 Socket API	7
4 VARMENTEIDEN KÄSITTELY	9
4.1 Laitevarmenteen hakeminen, toimittaminen ja sulkeminen	9
4.2 Varmennepyyntöjen ja varmenteiden muodot	9
4.3 Juurivarmentajan yksilöivät tiedot	10
4.4 Laitevarmentajan yksilöivät tiedot	10
4.5 Laitevarmenteen yksilöivät tiedot	10
5 TCP/IP-KATEVARMENNUSYHTEYDEN TESTAUS	12
5.1 Varmennussanomaliikenteen kuormitustestaus	12
5.2 Testauksen kohde	12
5.3 Testausprosessin kuvaus	13
5.3.1 Lähtötilanne	13
5.3.2 Testausprosessi	13
5.4 Lisätiedot	14
LIITE 1: TESTITAPAHTUMALUETTELO	15
LIITE 2: VPN -YHTEYSLOMAKE TESTAAJA – VARMENTAJA	16
LIITE 3 MAKSUPÄÄTETAHTUMIEN VÄLITYS AVOIMISSA VERKOISSA	17
1 JOHDANTO	17
2 MUUNNOS- JA VÄLITYSPALVELUIDEN TUOTTAMINEN	17
2.1 Välityspalvelun asiakasverkon suljettu käyttäjäryhmä	18
2.2 Visan ja MasterCardin PCI-vaatimusten täyttäminen	19
3 REITITYSLUPA JA -SOPIMUKSEN HAKEMINEN	19
LIITE 4: MAKSUPÄÄTEVARMENNEPALVELUN VARMENTEEN, SULKULISTAN JA HAKEMISTON KUVAUS	21



KATEVARMENNUS TCP/IP - YHTEYDELLÄ

1 JOHDANTO

Välitettävien tietojen luottamuksellisuus ja eheys suojataan julkisessa Internet-verkossa IPSec¹ standardin mukaisen vpn-tunnelin (Virtual Private Network) avulla. Lähettävät osapuolet tunnistavat toisensa IPSec-yhteyden avausvaiheessa X.509v3 standardin mukaisille laitevarmenteilla. Jokaisella varmennusverkkoon liittyvällä päätteellä tulee olla Varmennepalvelun antama laitevarmenne.

¹ IPsec avainkäsitteily ja yhteyden avausvaiheet on kuvattu dokumenteissa RFC 2406, 2407, 2408, 2409, 2412



2 SIIRTO-OTSAKE

Maksukorttitapahtuman varmennussanoma välitetään tcp/ip -yhteydellä "VASU"-siirto-otsakkeella varustettuna. Otsakkeella varustettua katevarmennussanomaa tai vastaus-sanomaa kutsutaan siirtosanomaksi. Otsake sisältää sanoman pituus tiedon, jonka avulla vastaanottaja voi poimia eri sanomat linjalta tulevasta tietovirrasta ja varmistua, että hän on vastaanottanut koko sanoman.

Tiedon numero	Nimi	Muoto	Selitys
1	SANOMATUNNUS	AN(4)	Vakio = "VASU"
2	VERSIO	AN(2)	Sanoman versio, aluksi = "01"
3	SANOMAN NRO	B(16)	Sanoman juokseva numero binaarisena
4	SANOMAN PITUUS	B(16)	Siirtosanomien pituus binaarisena

Taulukko 1. Siirto-otsake

- 1) Sanoman tunnus
Tietokenttä 1 (tavut 1 – 4) sisältää sanomatunnuksen, joka on vakio "VASU"
- 2) Versio
Tietokenttä 2 (tavut 5 ja 6) kertoo sanomakehyksen versiotiedon.. Versio-tieto muuttuu esimerkiksi laskenta-algoritmin tai sanomakehyksen rakenteen muutoksen yhteydessä.
- 3) Sanoman numero
Tietokenttä 3 (tavut 7 ja 8) sisältää binaarisen sanomalaskurin. Laskurin arvoa kasvatetaan yhdellä jokaisen lähetetyn sanoman jälkeen. Laskuria ei nollata välillä.
- 4) Sanoman pituus
Tietokenttä 4 (tavut 9 ja 10) ilmoittaa siirtosanomien pituuden tavuina.

Varsinainen maksupäätejärjestelmäkuvauksen mukainen katevarmennussanoma tai vastaussanoma liitetään välittömästi otsaketietojen jälkeen sellaisenaan.



3 TCP/IP YHTEYDET

3.1 Asiakkaan vpn-yhteys

Asiakkaan vpn-laitteella tulee olla julkinen ip-osoite ja se tulee olla tavoitettavissa julkisesta Internet-verkosta. Asiakkaan laite voi olla joko vpn-client tai vpn-gateway.

Asiakkaan tulee selvittää vpn-laitteensa tai -ohjelmistonsa yhteentoimivuus kortinmyöntäjien käyttämien vpn-yhdyskäytävän kanssa. Yhteentoimivuuteen liittyviä tietoja voi tiedustella pankista tai pankkien jakamista pankkikohtaisista dokumenteista.

Asiakkaan tulee varmistaa, että hänen vpn-laitteeseensa voidaan reitittää protokollat 50 (ESP), 51 (AH) ja sekä UDP portteihin 500 (IKE) ja 4500 (NAT-T). Huom. Protokollat 50 ja 51 ovat eri asia kuin portit 50 ja 51.

3.2 Sulkulistan tarkastus

Asiakkaan on tarkastettava varmenteiden voimassaolo sulkulistalta (CRL). Käytettävä sulkulista ei saa olla 15 minuuttia vanhempi.

Poikkeustilanteissa, joissa käytössä oleva sulkulista on vanhentunut eikä voimassaolevaa sulkulistaa saada Varmennepalvelusta, asiakkaan on voitava ohittaa CRL tarkastus tilapäisesti. Tarkastus on otettava käyttöön välittömästi Varmennepalvelun poikkeustilanteen mentyä ohi.

3.3 IPSec-yhteysparametrit

3.3.1 VPN-gateway

IKE/ISAKMP palvelinasetukset / MAIN MODE

- Käytössä Pankkien Varmennepalvelun laitevarmenne
- Tunnel mode
- Phase1
 - algorithms 3DES + SHA1
 - lifetime 3600 seconds, kilobytes not used (=0)
 - identities IPV4_SUBNET
 - Diffie-Hellman group 5
- Phase2
 - (ESP) algorithms 3DES + SHA1
 - lifetime 3600 seconds, kilobytes not used (=0)
 - identities IPV4_SUBNET
 - Diffie-Hellman group 5
 - PFS USED



3.3.2 VPN-client

IKE/ISAKMP asetukset

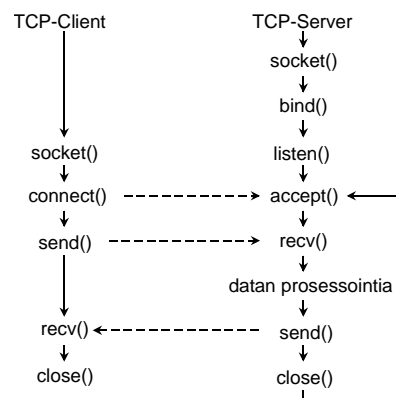
- Käytössä Pankkien Varmennepalvelun laitevarmenne
- Tunnel mode
- Phase1
 - algorithms 3DES + SHA1
 - lifetime 3600 seconds, kilobytes not used (=0)
 - identities IPV4_SUBNET
 - Diffie-Hellman group 5
- Phase2
 - (ESP) algorithms 3DES + SHA1
 - lifetime 3600 seconds, kilobytes not used (=0)
 - identities IPV4_SUBNET
 - Diffie-Hellman group 5
 - PFS USED
- Mahdollisuus käyttää NAT:ia
- PPTP- ja L2TP-protokollien käyttö ei ole mahdollista.

3.4 Socket API

Yhteys hoidetaan IPv4-version mukaisen stream-socket rajapinnan kautta, joka muodostaa tcp -yhteyden osapuolten välille. Varmennuskyselyn lähettäjä avaa tcp/ip -yhteyden, joka voi olla auki vain yhden varmennustapahtuma vaatiman ajan tai toistaiseksi.

- Socket-portin numero on 20333.
- Serverin time out on 90 s.
- Clientin time out on 30 s.

Seuraava kaavio 1 kuvaa yksinkertaisen istunnon vaiheet. Toteutuksesta riippuen, palvelimessa toiminta saattaa haarautua kunkin Accept-kutsun jälkeen omaksi prosessiksi / säikeeksi, joka hoitaa tapahtumakäsittelyn. Pääprosessi jää odottamaan seuraavaa kutsua.



Kaavio 1: Yksinkertainen istunto



Kutsu	Toiminto	Vastuutaho
socket()	luodaan socket TCP-yhteystavalle	Molemmat osapuolet
bind()	määrittelee socketin osoitteen	Varmentaja
listen()	hyväksyy yhteydenotot (connect)	Varmentaja
connect()	yhteydenotto palvelimeen	Asiakas
accept()	odottaa kutsua (connect)	Asiakas
send()	lähetä dataa	Molemmat osapuolet
recv()	lue dataa	Molemmat osapuolet
close()	sulje yhteys	Molemmat osapuolet

Taulukko2. Socket API:n ohjauskutsut

Esimerkin mukaisessa toimintamuodossa sanomat palvelaan yksitellen ja yhteyden avaukseen sekä sulkemiseen kuluu aikaa, jolloin serverin palvelun taso on huono kuormitetussa järjestelmässä. Jatkuva istunto toteutetaan siten, että serverin lähetettyä vastauksensa Send-palvelulla se palaa Recv-palveluun odottamaan seuraavaa sanomaa, mutta vain määrätyksi ajaksi. Kun client sulkee yhteyden, se aiheuttaa virheen serverin Recv-palvelulle, jolloin server sulkee yhteyden ja lopettaa prosessinsa/säikeensä.

Tietolohko voi pirstoutua siirtovaiheessa pienempiin lohkoihin, jotka socket API saattaa palauttaa erillisinä tietolohkoina sovellustason read-kutsuille. VASU-otsakkeessa olevan pituustiedon perusteella varmennuspyynnön vastaanottaja voi varmistua, että kaikki tieto tulee perille.



4 VARMENTEIDEN KÄSITTELY

Varmenteiden, sulkulistan ja hakemistopalvelun tarkempi kuvaus on liitteenä 4.

4.1 Laitevarmenteen hakeminen, toimittaminen ja sulkeminen

Varmenne haetaan hakijan tilikonttorista. Varmenne myönnetään hakijalle, jolla on voimassaoleva maksupäätöspalvelusopimus tai CA-neuvottelukunnan² tai sen valtuuttaman tahon kanssa tehty reitityspalvelusopimus.

Varmenteen hakija täyttää tilikonttorissa varmennehakemuksen, joka toimitetaan pankin rekisteröintipisteeseen. Rekisteröintipiste luo hakemuksen mukaisen varmenteen. Varmenteeseen mahdollisesti liittyvä PIN tunnus toimitetaan hakijalle postitse. Varmenne toimitetaan hakijan sopimuskonttoriin, joka voi olla joko tilikonttori tai hakemuksessa erikseen sovittu pankin konttori. PIN-kirjeessä oleva saate sisältää tiedon varmenteen noutoajankohdasta ja paikasta. Varmenne luovutetaan vain hakemuksessa mainitulle henkilölle. Hakijan on varauduttava henkilöllisyytensä todistamiseen.

Uusi varmenne myönnetään aikaisintaan 6 kk ennen edellisen varmenteen voimassaolon päättymistä. Pankki toimittaa varmenteen haltijalle ennakoilmoituksen varmenteen vanhenemisesta. Varmenteen uusinnassa menetellään samalla tavalla kuin ensimmäisen varmenteen noutamisessa.

Varmenteen haltija, katevarmennustapahtumia vastaanottava taho tai varmenteen myöntäjä voivat pyytää varmenteen suljettavaksi. Varmenne suljetaan ottamalla yhteyttä varmenteen myöntäneeseen pankkiin. Varmenteen sulkemisesta toimitetaan kirjallinen ilmoitus varmenteen haltijalle.

4.2 Varmennepyyntöjen ja varmenteiden muodot

Varmennepalvelu tukee menettelyjä, joissa RSA – avainpari luodaan pääsääntöisesti Pankkien Varmennepalvelun toimesta tai asiakkaan vpn – laitteessa siinä tapauksessa, että laite ei hyväksy muualla luotuja avaimia. Pankkien Varmennepalvelun tuottamat toimikorttivarmenteet ovat PKCS#15 muotoisia ja tiedostovarmenteet PKCS#12 muotoisia. Vpn – laitteen luoman varmennepyyntö tulee olla PKCS#10 muodossa. Varmennepalvelun varmenteiden ja sulkulistojen sisältö on kuvattu tarkemmin tämän dokumentin liitteessä 4.

Pankkien Varmennepalvelu tukee muistitikulla, toimikortilla, levykkeellä ja CD:llä toimitettavia varmenteita. Järjestelmässä käytettävät toimikorttien tyyppi on Setec Setcard 32k PKI³. Setec on toteuttanut kortin lukijaohjelmiston SetWeb.

Toimikortilla olevia avaimia ja niihin liittyvää varmennetta ei ole mahdollista siirtää kortilta järjestelmään. Kortti aktivoidaan PIN-tunnuksella ja avaimia käytetään kortilla. Tiedostomuotoiset avaimet ja varmenne on suojattu PIN-tunnuksella. Tietovälineellä olevat avaimet ja varmenne voidaan siirtää päätteen muistiin käyttöä varten. Yksityinen avain

² CA-neuvottelukunta on Pankkien Varmennepalvelun hallintoelin (ca-neuvottelukunta@pankkiyhdistys.fi)

³ www.setec.com.



on talletettava päätteeseen siten, ettei se paljastu sivullisille. Varmenteen ja avaimet sisältävä tietoväline on talletettava turvallisesti siten, etteivät ne joudu sivullisen haltuun.

Toimikortilla toimitettavien varmenteiden ja yksityisten avainten pituus on 1024 bittiä. Muilla tietovälineillä toimitettavien avainten pituus on 2048. Laitevarmenteen voimassaoloaika on kolme vuotta. Laitevarmenteita myöntävän Valmentajan varmenne on voimassa 10 vuotta.

Asiakkaan järjestelmän tulee tuke varmenteen käyttöön ja vaihtoon liittyvien toimenpiteiden lisäksi toimintoa, jolla varmenteen yksilöintitiedot ja voimassaoloaika voidaan selvittää.

4.3 Juurivarmentajan yksilöivät tiedot

Juurivarmentajan identiteetin yksilöintitietokenttien arvot ovat seuraavat:

Maatunnus (country, C)	= FI
Organisaation nimi (organisationName, O)	= SUOMEN PANKKIYHDISTYS RY
Yhteisnimi (commonName, CN)	= SUOMEN PANKKIYHDISTYS RY CA-Committee Root CA

4.4 Laitevarmentajan yksilöivät tiedot

Laitevarmentajan identiteetin yksilöintitietokenttien arvot ovat seuraavat:

Maatunnus (country, C)	= FI
Organisaation nimi (organisationName, O)	= SUOMEN PANKKIYHDISTYS RY
Yhteisnimi (commonName, CN)	= SUOMEN PANKKIYHDISTYS RY CA-Committee Device CA

Laitevarmentajan identiteettiin liitetyn lisätietokentän arvo:

IP-osoite (IPAddress)	= nnn.nnn.nnn.nnn
-----------------------	-------------------

4.5 Laitevarmenteen yksilöivät tiedot

Maksupäätteen ja maksupäätokeskittimen identiteetin yksilöintitietokenttien arvot muodostetaan seuraavasti:

Maatunnus (country, C)	= FI
Organisaation nimi (organisationName, O)	= Asiakkaan nimi
(Org.yksikön nimi (organisationalUnitName, OU)	= Asiakkaan yksikkö)
Laitenumero (serialNumber, SN)	= LLLYYYYYYYYYYYYNNNM
Yhteisnimi (commonName, CN)	= LLLYYYYYYYYYYYYNNNM

Yhteisnimi voi olla myös vpn-laitteen generoiman varmennepyynnön sisältämä FQDN tai ip-osoite.

IPSec-reitittimen identiteettiin liitetyn lisätietokentän arvo:

IP-osoite (IPAddress)	= nnn.nnn.nnn.nnn
-----------------------	-------------------

Organisaatioyksikön nimikenttä sisältää sen yrityksen ja yksikön yksikkötunnisteen, jonka hallinnassa maksupäätteen tai vpn-laite on. Laitenumeron ja yhteisnimen muodostaa ANS (19) -koodi, joka rakentuu neljästä osasta:

1. Rekisteröijän tunnus (3 numeroa etunollatäytöllä, LLL)
2. Maksupäätteen numero (12 numeroa, YYYYYYYYYYYY)
3. Maksupäätteen yksilöivä tunnus (3 numeroa, etunollatäytöllä, NNN)
4. Maksupäätteen tyyppi ja laitevarmenteen tyyppitunnuksen numeerinen arvo (1 numero, M)



MAKSUPÄÄTEVARMENTEEN TYYPPI	NUMEERINEN ARVO
Maksupäättevarmenne, varmentajan luoma avainpari	0
Maksupäättevarmenne, laitteen itse luoma avainpari	1
Reitityspalvelun IPSec-reititinvarmenne, varmentajan luoma avainpari	2
Reitityspalvelun IPSec-reititinvarmenne, laitteen itse luoma avainpari	3



5 TCP/IP-KATEVARMENNUSYHTEYDEN TESTAUS

5.1 Varmennussanomaliikenteen kuormitustestaus

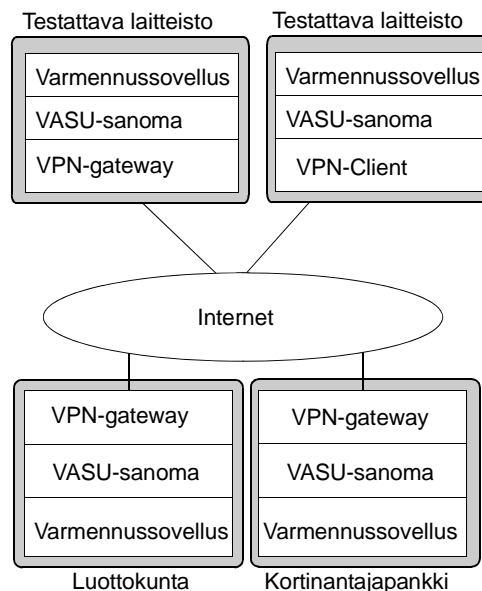
Jotta julkista tcp/ip – verkkoa käyttävät maksupäätteet ja kassajärjestelmät toimisivat yhteen uuden varmennusinfrastruktuurin kanssa, tulee ne testata tässä dokumentissa kuvatulla menettelytavalla ennen tuotantokäytön aloittamista. Kaikki tcp/ip - yhteydellä katevarmentajalle liikennöivät maksupäätte- tai yhdyskäytävälaitteet on testattava. Katevarmennussanomien käsittelyn ja sanomien sisällön oikeellisuus testataan EMV – päätelaitteiden osalta maksupäättehyväksyntään liittyvässä prosessissa.

Tämä dokumentti sisältää seuraaville testaajille tarkoitetut ohjeet:

- 1) Maksupäätte- ja kassajärjestelmätoimittajat
 - a. VPN yhdyskäytävä-yhdyskäytävä ja
 - b. VPN yhdyskäytävä-client –käyttötavat
- 2) Kaupat
 - a. VPN yhdyskäytävä-yhdyskäytävä – käyttötapa

5.2 Testauksen kohde

Testauksen kohteet on kuvattu oheisessa kaaviossa.



Testaus jakaantuu neljään osakokonaisuuteen:

1. VPN yhteyden muodostus IPSec – standardin mukaisesti.
2. TCP porttiyhteyden testaus
3. Varmennuksen pyyntö- ja vastaussanomien siirto-otsake (VASU)
4. Varmennussanomaliikenne (pyyntö, toisto, vastaus jne), jokaista kortinmyöntäjää vastaan.

Maksupäätteen tai yhdyskäytävä-laitteen toiminta testataan maksupäätteen ja katevarmennustapahtumien vastaanottajien välillä.

5.3 Testausprosessin kuvaus

5.3.1 Lähtötilanne

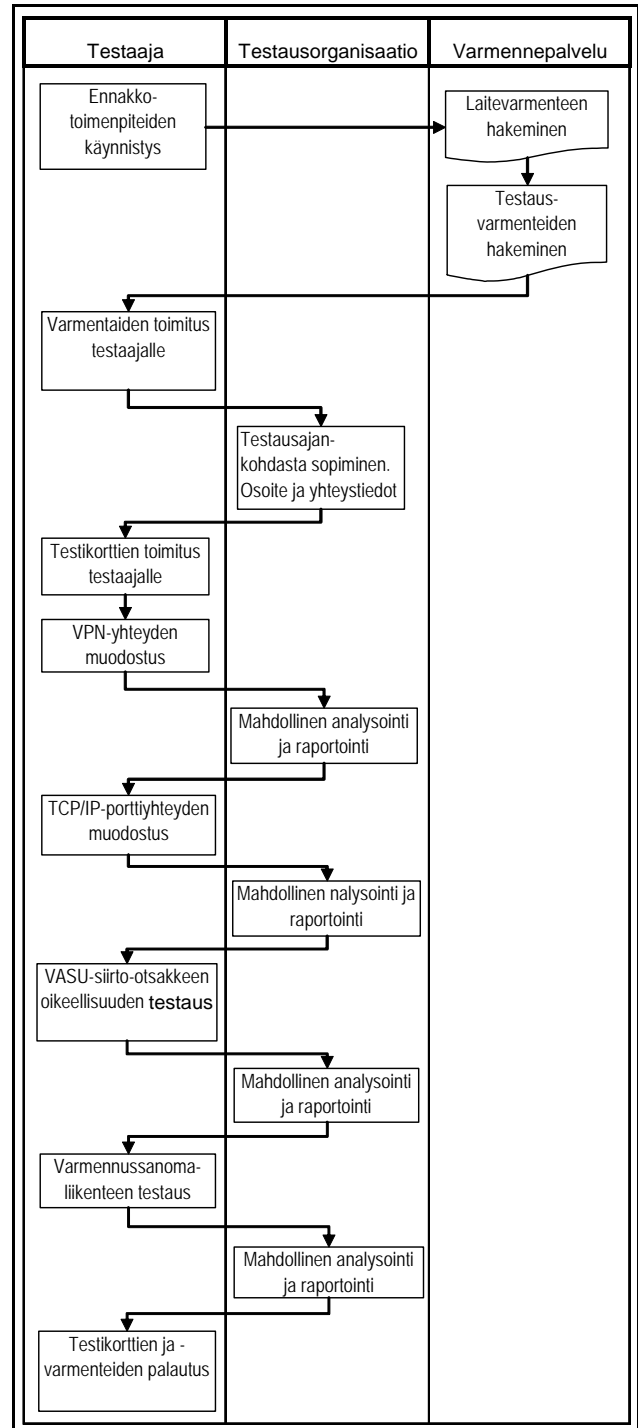
Maksupäätteen tai kassajärjestelmän vpn-clientilla tai vpn-yhdyskäytävällä tulee olla tcp/ip –katevarmennusverkkoon tarvittava Pankkien Varmennepalvelun myöntämä X.509v3 – muotoinen laitevarmenne ja testikortit, jotka Testaaja on ennakoon hankkinut tilipankiltaan.

Tässä kuvattu tietoliikenneyhteyden testaus voi olla osa maksupäätteen sertifiointiin liittyvää tarkastusprosessia tai se voi kohdistua aiemmin hyväksytyyn laitteen tcp/ip katevarmennusyhteyden testaukseen.⁴

5.3.2 Testausprosessi

Yhteydet on testattava jokaisen kortinmyöntäjän järjestelmää vastaa. Oheinen kaavio kuvaa testausprosessia, joka etenee seuraavasti:

- 1) Halutessaan testata TCP/IP – varmennusta maksupäätte- / kassajärjestelmätoimittaja hankkii tarvittavat laitevarmenteet ja ennen testausta ottaa hyvissä ajoin (> 1kk) yhteyden Luottokuntaan ja kortinmyöntäjäpankkiin sopiaukseen testauksen ajankohdasta ja testaukseen liittyvistä asioista.
- 2) Testaaja toimittaa testausosapuolille osoite ja yhteyshenkilötietonsa, tilaa kortinmyöntäjiltä testikortit sekä esittää toiveen halutusta testausajankohdasta.



⁴ Käyttöön otettavan EMV – maksupäätteen tai -kassajärjestelmän tulee olla EMV-sertifioitu. Magneettijuovateknologiaan pohjautuvan maksupäätteen tulee olla pankkien hyväksymä.



Testikortteja tulisi olla vähintään viisi kappaletta, jos yhteyttä testataan yhden kortinmyöntäjän kanssa. Kortteja voi olla yksi/testausosapuoli, kun yhteyksiä testataan rinnakkain useamman kortinantajan kanssa. Tällöin yhteyttä testataan vuorotellen eri osapuolten kanssa.

- 3) Luottokunta ja kortinmyöntäjät toimittavat tarvittavat testikortit, testitapahtuma luette-
lon sekä ilmoittavat testin ajankohdan testaajalle sekä järjestävät testausistunnon
sovittuna ajankohtana.
- 4) Testaaja suorittaa sovitut testitapahtumat ja testausosapuolet tarkastavat testien oi-
keellisuuden. Testitapahtumat on lueteltu oheisessa liitteessä 1.
- 5) Kukin testausosapuoli voi tapauksesta riippuen, pyydettyä antaa raportin testien
analysoinnista.
- 6) Testaaja palauttaa testikortit ja testivarmenteet niiden toimittajille.

Testaustapahtuma on kertaluonteinen, kontrolloitu tapahtuma, jonka ajaksi testaajalle on
avattu pääsy Luottokunnan ja kortinmyöntäjän testausympäristöön. Tämä pääsyoikeus
lopetetaan testaustapahtuman päätteeksi. Vapaamuotoinen testaaminen ei ole mahdol-
lista.

5.4 Lisätiedot

Lisätietoja asiasta saa asianomaisten organisaatioiden www-sivuilta sekä:

- Finanssialan Keskusliitto: www.fkl.fi
- Pankkien Varmennepalvelu: www.fba-ca-committee.fi



LIITE 1: TESTITAPAHTUMALUETTELO

1) Vpn-yhteyden muodostus ja varmenteiden käsittely

a) Asiakkaan omat varmenteet:

- Yhteyden muodostuminen voimassaolevalla varmenteella
 - Tunnistautuminen ja salakirjoitetun yhteyden avaus varmenteella
- Sulkulistan käsittely
 - Yhteyden testaus suljetulla varmenteella

b) Katevarmentajan varmenteet

- Yhteyden muodostuminen voimassaolevalla varmenteella
 - Tunnistautuminen ja salakirjoitetun yhteyden avaus varmenteella
- Sulkulistan käsittely
 - Yhteyden testaus suljetulla varmenteella

2) Porttiyhteyden muodostus

3) VASU-siirto-otsikon oikeellisuus

4) Katevarmennusyhteyden testaus

Varsinainen katevarmennusyhteys testataan, kun edellisissä kohdissa olevat vaiheet on todettu toimiviksi. Testattavat tapahtumat ovat Katevarmennus ja Varmennuksen peruutus, jota toteutetaan vuoronperään.



LIITE 2: VPN -YHTEYSLOMAKE TESTAAJA – VARMENTAJA

IPSec VPN yhteystiedot _____ (Testaajan) ja
_____ (Varmentajan) välille.

Tavoiteltu testaus päivä: ____ . ____ 200__

Testaajan yhteystiedot:

Yrityksen nimi _____

Lähiosoite _____

Postitoimipaikka _____

Yhteyshenkilön nimi _____

Puhelinnumero _____

Sähköposti _____

Varmentaja → Testaaja			
Lähdeosoite ja verkkomaski	Kohdeosoite ja verkkomaski	Portti/palvelu	kommentteja
		20333 tcp	

VPN päätepiste:

Varmentaja: IP-osoite: _____

VPN-laite: _____

Ohjelmisto: _____

Testaaja: IP-osoite: _____

VPN-laite: _____

Ohjelmisto: _____

Paikka: _____ Päiväys: ____ . ____ 200__

Allekirjoitus: _____

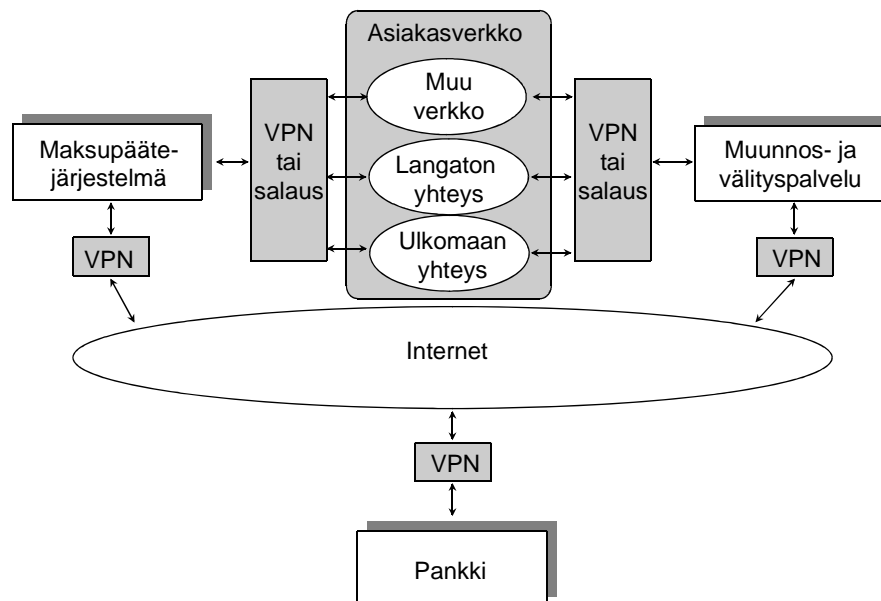
Nimen selvennys:

LIITE 3 MAKSUPÄÄTETAPAHTUMIEN VÄLITYS AVOIMISSA VERKOISSA

1 JOHDANTO

Liite kuvaa maksupäättevarmennusten ja -tapahtumien välityksessä noudatettavat tietoturva-periaatteet, kun tapahtumat välitetään avointen verkkojen kautta tai välityksessä käytetään välitys- ja muunnospalvelua.

Vaativuutena on, että kaikki pankkiaineistoja sisältävä tietoliikenne langattomissa ja julkisissa Internet verkoissa sekä ulkomaan yhteyksillä salakirjoitetaan. Salakirjoitus on toteutettava vahvalla salakirjoitustekniikalla. Wlan-, gsm- ja gprs-järjestelmien käyttämät menetelmät eivät sellaisenaan ole riittäviä ja asiakasverkon salauksen on ulotuttava siirtoyhteyden päästä päähän. Vaatimus koskee myös niitä tilanteita, joissa muunnos- ja välityspalvelusta tapahtumat välitetään X.25 suljetun katevarmennusverkon kautta pankkeihin.



Kuva 1. Palvelun toimintaympäristö

Pankin ja maksupäätetapahtumia välittävän osapuolen välinen VPN-yhteys muodostetaan Pankkien Varmennepalvelun myöntämällä laitevarmenteilla.

Välitys- ja muunnospalvelu saa kytkeä VPN-yhteydelle vain osapuolia, joilla on voimassa oleva maksupäättesopimus jonkin maksupäättepalvelua tarjoavan pankin kanssa.

2 MUUNNOS- JA VÄLITYSPALVELUIDEN TUOTTAMINEN

Maksupäätetapahtumien välittäminen muunnos- ja välityspalvelun kautta pankkeihin edellyttää palvelun tuottajalta reititysopimusta, jonka hakemiseen liittyvät asiat on kuvattu ohessa.



2.1 Välityspalvelun asiakasverkon suljettu käyttäjäryhmä

Palvelun tuottajan on toimitettava Finanssialan Keskusliittoon selvitys palvelussa noudatettavista peruseriaa-asteista. Selvitykseen liitettävät tiedot on lueteltu ohessa.

1. Välitys- ja muunnospalvelun tuottajan tiedot

- Palvelun tuottajan, hallinnoijan ja yhteyshenkilön yhteystiedot

2. Palveluntuottajan asiakasverkon osapuolet

- Tuotetaanko palvelua omalle kauppiaaryhmälle?
 - Selvitys kauppiaaryhmän rakenteesta
- Myydäänkö palvelua kolmansille osapuolille?
 - Selvitys niistä kriteereistä ja menettelyistä, joita noudatetaan, kun uusia osapuolia liitetään muunnospalveluun.

3. Asiakasverkon valvonta

Palvelun tuottajan tulee poistaa asiakasverkosta häiritsevä tai ehtoja rikkova osapuoli joko itse havaitsemansa häirinnän takia tai pankin pyynnöstä.

- Miten palvelun tuottaja valvoo verkkoa mahdollisten häirintätilanteiden ja muiden rikkomusten varalta?
- Yhteystiedot pisteestä, jonne pankki voi ilmoittaa pyynnön palveluun liitetyn asiakkaan poissulkemiseksi?

4. Palvelun osapuolten tunnistaminen

Palveluntuottajan tulee tietää, että asiakasverkon tapahtumat tulevat palvelun käyttöön oikeutetulta päätelaitteelta.

- Miten palvelu tunnistaa asiakasverkossa olevat päätelaitteet?

5. Tietojen salakirjoitus

Avoimissa tai langattomissa verkoissa liikkuvat tiedot on salakirjoitettava ja salaukseen käytetyt avaimet tulee vaihtaa aika-ajoin. Turvallisuusvaatimukset vastaavat periaatteessa IPsec-standardin mukaista vpn-yhteyttä ja siihen liittyvää CA-toimintaa.

Mitkä ovat palvelun asiakasverkossa käytettävät:

- Salakirjoitusmenettelyt ja siirtokäytännöt?
- Käytetyt algoritmit ja avainpituudet?
 - Symmetristen algoritmien avainten pituus oltava vähintään 128 bittiä
 - RSA avainten pituudet oltava vähintään 1024 bittiä



- Avainhallinnon periaatteet?

6. Verkkoratkaisun arkkitehtuurikuva

Hakemukseen on liitettävä graafinen kuva palvelun verkkoympäristön rakenteesta täydennettynä lyhyellä sanallisella kuvauksella.

2.2 Visan ja MasterCardin PCI-vaatimusten täyttäminen

Reitityspalvelun tulee täyttää VISA:n ja MasterCardin julkaiseman PCI-standardin vaatimukset. Hakemuksen liitteeksi tulee toimittaa PCI itsearviointi, mikäli hakija ei vielä täytä PCI yhteensopivuusvaatimuksia.

PCI-standardiin liittyvät tiedot on noudettavissa osoitteista:

<http://www.visaeurope.com/acceptingvisa/ais.html>

<https://sdp.mastercardintl.com>

3 REITITYSLUPA JA -SOPIMUKSEN HAKEMINEN

Edellisten tietojen lisäksi hakijan tulee toimittaa Finanssialan Keskusliittoon omilla tiedoillaan täydennetty reitityssopimuskaavake. Kaavake on seuraavalla sivulla. Hakemuksen käsittely ja reitityssopimuksen tekeminen etenee seuraavan prosessin mukaisesti.

- 1) Hakija toimittaa täytetyn kaavakkeen ja edellä mainitut tiedot osoitteella

Finanssialan Keskusliitto
Tietoturvallisuusjaoston sihteeri
Bulevardi 28
00120 Helsinki

- 2) Pankkien yhteistyöelimet käsittelevät hakemuksen ja antavat lausuntonsa.

Hakemukset käsitellään normaalisti 1 -2 kk välein kokoontuvissa Finanssialan keskusliiton toimielimissä. Hakemukset käsitellään luottamuksellisesti.

- 3) Hyväksytyyn hakemukseen liittyvät kaavake toimitetaan käsittelytiedoilla täytettynä hakijalle. Jos hakemus hylätään, niin hakijalla toimitetaan tiedot hyläyksen syystä.
- 4) Hakija menee em. täydennetyn kaavakkeen kanssa pankkiinsa.
- 5) Pankki tunnistaa hakijan ja hoitaa reitityssopimukseen viralliset allekirjoitukset
- 6) Pankki hoitaa varmennehakemuksen ja varmenteen toimittamiseen liittyvät asiat.



SOPIMUS MUUNNOS- JA REITITYSPALVELUN ASIAKKAIDEN MAKSUPÄÄTETAHTUMIEN REITITTÄMISESTÄ PANKKEIHIN JA LUOTTOKUNTAAN			
Hakija	Yrityksen nimi	Y-tunnus	
Hakijan yhteyshenkilö	Yhteyshenkilön nimi	Puhelinnumero	
	Lähiosoite / postilokero	Telekopio	
	Postitoimipaikka	Sähköpostiosoite	
Liittämisen ehdot	<p>Hakija sitoutuu siihen, että se reitittää pankkien ja Luottokunnan maksupääteläveluun vain sellaisten palvelunsa käyttäjensä tapahtumia, joilla on</p> <ul style="list-style-type: none">voimassaoleva maksupäätelävelusopimus pankkinsa kanssa,käytössään Suomessa käytettäväksi hyväksytty maksupäätelä jaHakijan sisäisen tietojärjestelmän käyttöoikeus jajoita täyttävät VISA:n ja MasterCardin PCI-DSS standardin auditointi- ja skannausvaatimukset <p>Palvelun käyttäjä saa välittää Hakijan reitityspalvelun kautta ainoastaan maksukorttien takuuehtojen mukaisia ja pankkien ja Luottokunnan määrittelemien maksupääteläjärjestelmävausten sekä varmennusstandardin mukaisesti toimivien maksupääteläiden tekemiä tapahtumia.</p> <p>Hakija vastaa virheellisten varmennusten aiheuttamista vahingoista.</p>	<p>Väärinkäytöstapauksissa Hakijalla on velvollisuus poistaa väärinkäyttäjät reitityspalvelustaan joko heti havaittuaan väärinkäytökset tai pankkien tai Finanssialan keskusliiton pyynnöstä</p> <p>Pankeilla tai Luottokunnalla on oikeus saada välitystapahtumiin liittyviä tietoja Hakijan reitityspalvelun kautta tehdyistä tapahtumista, jos perusteltua tarvetta ilmenee.</p> <p>Pankeilla on oikeus irtisanoa tämä sopimus, jos Hakijan tietojärjestelmät eivät läpäise PCI-standardin mukaista auditointia.</p> <p>Hakija sitoutuu toimittamaan vuosittain tai erikseen CA-Neuvottelukunnan pyynnöstä tiedot niistä palvelun käyttäjistään, jotka se on yhdistänyt asiakasverkkonsa kautta pankkeihin ja Luottokuntaan.</p> <p>CA-Neuvottelukunnalla on oikeus pankkien tai Luottokunnan pyynnöstä peruuttaa Hakijan valtuutus reitittää palvelunsa käyttäjien tapahtumia ja pyytää Hakijan laitevarmenteen sulkemista Pankkien Varmennepalvelussa.</p>	
VISA:n ja MasterCardin PCI-DSS vaatimukset	a) itsearviointi () valmis, () valmistuu pvm ___/___/200___ b) auditointi- ja skannausvaatimukset () käynnistynyt, () käynnistyy pvm ___/___/200___ Lisätieto:		
Hakijan allekirjoitus	Hakija sitoutuu noudattamaan CA-Neuvottelukunnan hallinnoiman Pankkien Varmennepalvelun varmenteiden käyttöön liittyviä ehtoja, pankkien, Finanssialan keskusliiton tai Luottokunnan antamia maksupäätelävelun käyttöön liittyviä ohjeita.		
	Paikka ja aika	Hakijan allekirjoitus ja nimen selvennys	
Finanssialan keskusliiton tietoteknisen turvallisuusjaoston käsittely	() Hyväksytty pvm. () Hylätty pvm. Syy:	Allekirjoitukset ja nimen selvennykset	
CA-Neuvottelukunnan valtuuttaman tahon allekirjoitus	Paikka ja aika	Allekirjoitukset ja nimen selvennykset	
Hakijan allekirjoitus sopimuskonttorissa	Pankin konttori	Hakijan allekirjoitus ja nimen selvennys	
Pankin allekirjoitus	Hakijan tunnistusasiakirja	Päivämäärä	Pankin yhteyshenkilö
	Ajokortti		
	Henkilökortti		
	Passi		
	Tunnettu		



LIITE 4: MAKSUPÄÄTEVARMENNEPALVELUN VARMENTEEN, SULKULISTAN JA HAKEMISTON KUVAUS.