



**PATU
PANKKIEN ASIAKASYHTEYKSIEN
TIETOTURVA
TIEDOSTOSIIRRON SUOJAAMINEN**

**OSA 1:
TODENTAMISEN JA EHEYDEN-
VALVONNAN MENETELMÄT
SEKÄ AVAINTEN HALLINTA**

Versio 1.22
10.9.1998

Tämä dokumentti toimii pankkien järjestelmäsuunnittelun lähtökohtana
eikä kuvaa pankkikohtaisia ratkaisuja.



MUUTOSLUETTELO

| <u>Versiotunnus</u> | <u>Luku-Sivu</u> | <u>Huom.</u> |
|---------------------|------------------|--|
| V 1.1 | kaikki sivut | |
| V 1.11 | M - 1 | |
| V 1.11 | Liite 3 | Korjattu MAC-laskennan lopputulokset |
| V 1.2 | kaikki sivut | |
| V 1.21 | M - 1 | |
| V 1.21 | 4 - 2 | ESIp-sanoman käsittely |
| V 1.22 | Kaikki | Dokumentti on siirretty toiseen tekstinkäsittelyohjelmistoon |

HYVÄKSYMINEN

| <u>Versiotunnus</u> | <u>Päivämäärä</u> | <u>Hyväksyjä</u> |
|---------------------|-------------------|----------------------------------|
| V 1.0 | 23.4.1992 | Maksuliikennetoimikunta |
| V 1.1 | 19.11.1992 | Tietotekninen turvallisuusjaosto |
| V 1.11 | 31.12.1992 | Tietotekninen turvallisuusjaosto |
| V 1.2 | 16.3.1994 | Tietotekninen turvallisuusjaosto |
| V 1.21 | 17.3.1995 | Tietotekninen turvallisuusjaosto |
| V 1.22 | 17.8.1998 | Tietotekninen turvallisuusjaosto |



MUUTOKSET EDELLISEEN VERSIOON

Tämä dokumentti on päivitetty edelliseen PATUn versioon (V 1.21) tulleiden palautteiden perusteella. Tässä päivityksessä ei ole varsinaiseen suojausmenettelyyn liittyviä muutoksia.

PATUN KÄYTTÖÖNOTTOAIKATAULUT

Tässä dokumentissa kuvattu PATU -menettely on kokonaisuudessaan käytössä. Asiakkaan todennusta käytetään aina, mutta aineistojen eheyden suojaamisesta asiakas ja pankki sopivat keskenään. Erillisenä kuvauksena oleva aineistojen salakirjoitus ei ole käytössä.



| | | |
|-------|--|-----|
| 1 | JOHDANTO..... | 1 |
| 1.1 | Yleistä..... | 1 |
| 1.2 | Liittyvät standardit ja suositukset..... | 1 |
| 2 | KÄSITTEITÄ..... | 2-1 |
| 3 | MENETELMÄN KUVAUS..... | 3-1 |
| 3.1 | Yleistä..... | 3-1 |
| 3.1.1 | DES-algoritmi..... | 3-1 |
| 3.1.2 | Osapuolet..... | 3-1 |
| 3.1.3 | Asiakasjärjestelmien työnkulku..... | 3-1 |
| 3.1.4 | Tietoturva vaatimukset..... | 3-1 |
| 3.1.5 | Turvasanomien..... | 3-1 |
| 3.2 | Pankin ja asiakkaan todentaminen..... | 3-2 |
| 3.3 | Siirto- ja aineistoerän suojaaminen..... | 3-2 |
| 3.4 | Suojatun erän vastaanoton varmistaminen..... | 3-2 |
| 3.5 | Välittäjän ja omistajan tekemät suojaukset..... | 3-2 |
| 3.5.1 | Palveluverkon ja palvelukeskuksen rooli..... | 3-2 |
| 3.5.2 | Aineiston suojaus..... | 3-3 |
| 3.5.3 | Suojauksessa käytettävä avain..... | 3-3 |
| 3.5.4 | Suojattava kokonaisuus..... | 3-3 |
| 3.5.5 | Sopimukset..... | 3-4 |
| 4 | TURVASANOMAT JA NIIDEN KÄYTTÖ..... | 4-1 |
| 4.1 | Turvasanomien tiedot..... | 4-1 |
| 4.2 | Tietojen käyttö eri turvasanomissa..... | 4-1 |
| 4.3 | Pankin ja asiakkaan todentaminen..... | 4-2 |
| 4.3.1 | Esittäytyminen yhteydellisessä tiedostosiirrossa..... | 4-2 |
| 4.3.2 | Esittäytyminen yhteydettömässä tiedostosiirrossa..... | 4-2 |
| 4.3.3 | Pankin suorittamat tarkastukset..... | 4-2 |
| 4.3.4 | Asiakkaan suorittamat tarkastukset..... | 4-2 |
| 4.4 | Aineistoerien suojaaminen..... | 4-2 |
| 4.4.1 | Aineistoerien suojaaminen yhteydellisessä tiedostosiirrossa..... | 4-2 |
| 4.4.2 | Aineistoerien suojaaminen yhteydettömässä tiedostosiirrossa..... | 4-3 |
| 4.4.3 | Pankin tarkastukset SUO- ja VAR-sanomille..... | 4-3 |
| 4.4.4 | Asiakkaan tarkastukset PTE-sanomalle..... | 4-4 |
| 4.4.5 | Asiakkaan tarkastukset SUO- ja VAR-sanomille..... | 4-4 |
| 4.5 | Turvasanomien jakomenettely..... | 4-5 |
| 4.5.1 | Käsittelysäännöt..... | 4-5 |
| 4.5.2 | Esimerkkejä turvasanomien jakamisesta..... | 4-6 |
| 5 | TIIVISTEEN JA TARKISTEEN MUODOSTAMINEN..... | 5-1 |
| 5.1 | Tiivisteen muodostaminen..... | 5-1 |
| 5.1.1 | Kerta-avaimen muodostaminen..... | 5-1 |
| 5.1.2 | Käsiteltävä aineistoerä..... | 5-1 |
| 5.1.3 | Tietueraja ja aineistoerän loppu..... | 5-1 |
| 5.1.4 | Tiiviste..... | 5-1 |
| 5.2 | Tarkisteen muodostaminen..... | 5-1 |
| 5.3 | Kerta-avaimen muodostaminen..... | 5-1 |
| 5.4 | Sisäinen koodi..... | 5-2 |
| 5.5 | MAC-laskenta..... | 5-2 |
| 6 | AVAINHALLINTO..... | 6-1 |
| 6.1 | Yleistä..... | 6-1 |
| 6.1.1 | Avaintyytit..... | 6-1 |
| 6.1.2 | Avaimen sukupolvinumero..... | 6-1 |
| 6.1.3 | Avainten pariteetti..... | 6-1 |
| 6.1.4 | Avaintarkiste..... | 6-1 |
| 6.2 | Avainten jakelu ja vaihto..... | 6-2 |



| | | |
|-------|--|-----|
| 6.2.1 | Siirtoavaimen jakelu..... | 6-2 |
| 6.2.2 | Siirtoavaimen syöttö..... | 6-3 |
| 6.2.3 | Käyttöavaimen vaihto..... | 6-4 |
| 6.2.4 | Asiakkaan pyytämä käyttöavaimen vaihto | 6-4 |
| 6.2.5 | Vaihtojakson katkaiseminen | 6-5 |
| 6.3 | Turvamenetelmien käyttöönottoon liittyvät toimenpiteet | 6-5 |
| 7 | ILMOITUSKODIT | 7-1 |

LIITTEET:

1. Turvasanomien tiedot
2. Turvasanomissa käytettävät tietokentät
3. Esimerkki turvasanomien käytöstä ja sisällöstä



PATU

PANKKIEN ASIAKASYHTEYKSIEN TIETOTURVA TIEDOSTOSIIRRON SUOJAAMINEN OSA 1

1 JOHDANTO

1.1 Yleistä

Sähköisiä pankkipalveluita käytettäessä on yhteyden osapuolilla tarve todentaa toisensa varmalla tavalla sekä varmistaa aineistoerien eheys (muuttamattomuus) tiedonsiirron aikana. Asiakkaalla on lisäksi tarve saada kuittaus pankilta lähettämiensä aineistoerien vastaanottamisesta.

Pankkien tiedonsiirtoyhteyksien tietoturvamenetelmä PATU sisältää edellä mainitut turvatoiminnot. PATU kattaa yritysten ja yhteisöjen sekä pankin välisten aineistojen suojauksen.

PATU perustuu ISO 8730 ja ISO 8731-1 standardien mukaiseen tarkistusenttämennetelmään eli MACiin (Message Authentication Code). Menetelmä on toteutettavissa useimpiin pankkien asiakkaiden käyttämiin ohjelmoitaviin tietojärjestelmiin.

Kuvaus on laadittu Suomen Pankkiyhdistyksen tietoteknisen turvallisuusjaoston ja maksuliikenne toimikunnan asiakasyhteyksien turvatyöryhmissä.

Turvamenetelmän pankkikohtaiset soveltamisohjeet on esitetty kunkin pankin omissa tiedostosiirron kuvauksessa.

1.2 Liittyvät standardit ja suositukset

ANSI X3.92-1981,
American National Standard for Data Encryption Algorithm

ANSI X3.106-1983,
American National Standard for Information Systems - Modes Of Operation.

ISO 8730,
Banking - Requirements for Message Authentication (Wholesale)

ISO 8731-1,
Banking - Approved Algorithms for Message Authentication - Part 1: DEA

SFS 5748,
Organisaatioiden välinen tiedonsiirto (OVT), OVT-tunnus

Nämä standardit on saatavilla Suomen Standardisoimisliitto SFS:n myyntipisteestä.



2 KÄSITTEITÄ

Aineistoerä

Aineistoerä on pankin palvelukuvauksen mukainen sarja sanomia, jotka muodostavat kokonaisuuden. Aineistoerä on aina yhtä aineistotyyppiä ja on yhden asiakkaan aineistoa. Monella aineistotyyppillä aineistoerä alkaa erätietueella ja loppuu summatietueeseen.

Aineistotyyppi

Pankkipalveluaineiston tyyppi, joita ovat esimerkiksi toistuvaissuoritusaineisto, laskujen maksupalveluaineisto, tapahtumaluettelo, tiliote, jne.

Asiakas

Asiakas on osapuoli, joka tekee pankin kanssa sopimuksen PATUN käytöstä ja jolle pankki toimittaa PATUN siirtoavaimet. Asiakas voi olla omistaja-asiakas tai välittäjä-asiakas.

Avaaminen

Salakirjoitetun tiedon muuttaminen selväkieliseksi.

Avain

Salakirjoitusalgoritmin parametri, joka määrää muunnoksen selväkielisestä salakirjoitetuksi tiedoksi. Tämän standardin avaimet ovat DES-avaimia eli DES-algoritmin avaimia.

Avaimen vaihtojakso

Aika uuden avaimen voimassaolon alkamispäivästä edellisen avaimen voimassaolon päättymispäivään.

Binäärinolla

Tieto, jonka jokaisen bitin arvo on nolla.

DES-algoritmi

DES-algoritmi on ANSI X3.92-1981 standardin mukainen symmetrinen salakirjoitusalgoritmi, jossa tiedon salaamiseen ja avaamiseen käytetään samaa

avainta. DES-algoritmia kutsutaan myös DEA-algoritmiksi.

DES-avain

DES-algoritmin yhteydessä käytettävä avaintieto, joka on 64 bittiä pitkä. Kunkin tavun vähiten merkitsevät bitit ovat tavukohtaisia pariteettibittejä. Avaimessa käytetään paritonta pariteettia.

Exclusive OR -operaatio (XOR)

Binäärinen bittikohtainen yhteenlasku.

Fyysinen sanoma

Siirrettävä kokonaisuus on fyysinen sanoma ja se noudattaa tietoliikenteen tai aineistotyyppin asettamaa ylärajaa.

Heksadesimaaliesitys

Kuusitoistajärjestelmän mukainen lukujen esitystapa, jossa numerojärjestelmän kantaluku on 16. Numerojärjestelmän muodostavat numerot 0-9 ja kirjaimet A - F. Numerot voidaan esittää neljän bitin binäärilukuna seuraavan taulukon mukaisesti.

| | | | | | | | |
|------|---|------|---|------|---|------|---|
| 0000 | 0 | 0100 | 4 | 1000 | 8 | 1100 | C |
| 0001 | 1 | 0101 | 5 | 1001 | 9 | 1101 | D |
| 0010 | 2 | 0110 | 6 | 1010 | A | 1110 | E |
| 0011 | 3 | 0111 | 7 | 1011 | B | 1111 | F |

Kryptografia

Oppi salakirjoitusmenetelmistä ja niihin perustuvista tiedon suojausmenetelmistä.

Linjasiirto

Tiedonsiirto tietoliikenneyhteyden kautta.

Looginen sanoma

Looginen sanoma on kohdassa 4 olevan sanomakuvauksen mukainen, kiinteänpituisen sanoma. Alussa on loogisen sanoman pituus. Tämä pituus kattaa sanomatyyppin sanomakuvauksessa olevat kentät.



MAC, Message Authentication Code

ISO 8731-1 standardin mukaisesti aineistoerästä laskettu tarkistetieto. Menetelmä käyttää DES-algoritmia ja siinä käytetään salaista DES-avainta.

Omistaja-asiakas

Omistaja-asiakkaaksi kutsutaan osapuolta, joka on pankin tiliasiakas ja jonka aineistoerästä on kyse.

Pankki

Pankki on toinen osapuoli on, joka sopii asiakkaan kanssa PATUN käyttöön otosta ja toimittaa asiakkaalle PATUN käyttöön liittyvät siirtoavaimet.

Pariteetti

Tiedon ykkösbittien lukumäärää kuvaava, yhdellä bitillä ilmoitettu ominaisuus. Pariteettibitillä merkin ykkösbittien määrä säädetään joko parilliseksi (=parillinen pariteetti) tai parittomaksi (=pariton pariteetti).

Salakirjoittaminen, salaus

Selväkielen muuttaminen salaamismenetelmää käyttäen salakieleksi. Salaamiselle on yleensä olemassa käänteismuunnos (= avaaminen) salakielen muuttamiseksi selväkieliseksi.

Siirtoerä

Yhdellä kerralla lähetettävä kokonaisuus, joka voi sisältää yhden tai useita aineistoeräiä.

Sisäinen koodi

Merkkikoodisto, jota käytetään PATUn MAC-laskennassa. Koodisto tekee MAC-laskennan tuloksen aineistossa käytettävästä merkkikoodista riippumattomaksi (esim. ASCII tai EBCDIC).

Sovellusanoma

Yhteydellisessä tiedostosiirrossa käytetty sanoma, jolla asiakkaan järjestelmä ilmoittaa pankin järjestel-

mälle, että se seuraavaksi lähettää aineistoerän, tai että se odottaa pankilta saavansa aineistoerän.

Tarkiste

Turvasanomien osasta laskettu MAC, joka on laskettu käyttöavaimella.

Tiedostosiirto eli eräsiirto

Ennalta muodostetun aineistokokonaisuuden lähettäminen tiedostomuodossa. Vastakohtana on merkki kerrallaan tapahtuva siirto.

Tiiviste

Aineistoerästä laskettu MAC, joka on laskettu kertaavaimella.

Todennus

Todennus on tunnistuksen varmistamista. Todennuksessa vastapuoli varmistaa riittävällä varmuudella esittäytyvän osapuolen 'henkilöllisyyden'.

Välittäjä-asiakas

Välittäjäasiakas on palvelukeskus tai palveluverkko, joka toimii omistaja-asiakkaan toimeksiannosta.

Yhteydellinen tiedostosiirto
(l. vuorovaikutteinen, connected)

Yhteydellistä siirtoa kutsutaan usein linjasiirroksi. Yhteydellisessä tiedostosiirrossa asiakkaan ja pankin sovellukset keskustelevat keskenään. Asiakas muodostaa yhteyden pankkiin tiedostosiirtoa varten. Siirto voi suuntautua asiakkaalta pankkiin tai päinvastoin.

Yhteydetön tiedostosiirto
(l. vuorovaikutukseton, connectionless)

Yhteydetön tiedostosiirrossa asiakas ja pankki lähettävät toisilleen tiedostoja ilman sovellusohjelmien vuorovaikutusta siirron aikana. Tällainen siirtotapa on esimerkiksi välivarastoiva tiedonsiirto.



3 MENETELMÄN KUVAUS

3.1 Yleistä

3.1.1 DES-algoritmi

PATUn turvamenetelmä perustuu DES-algoritmiin ja salaisten avainten käyttöön ja toteuttaa seuraavat toiminnot:

- asiakkaan ja pankin todentaminen
- aineistoerän suojaaminen muuntumiselta
- aineistoerän vastaanoton varmistaminen

Tässä PATUn versiossa käytetään DESillä laskettavaa MAC-tarkistekenttää, joka liitetään suojattavan aineistoerän mukaan. Aineistoerää ei voida muuttaa ilman, ettei siitä laskettu MAC-tarkiste muutu. Oikeata MACia ei pysty laskemaan tuntematta laskennassa käytettävää avainta. PATUssa MAC lasketaan kahdesti ja vastaavia tarkistuskenttiä kutsutaan TII-VISTEeksi ja TARKISTEeksi.

Yhteydellisen ja yhteydettömän tiedostosiirron turvamenetelmät ovat samanlaisia. Tarkistuskentät ja muut tiedot on koottu omiksi sanomatyypeiksi, turvasanomiksi.

3.1.2 Osapuolet

Osapuolet tunnistetaan turvasanomien tietoryhmien LÄHETTÄJÄ ja VASTAANOTTAJA avulla. Tietoryhmät koostuvat kahdesta tiedosta, jotka ovat TUNNUS ja TARKENNE.

Tunnuksella, jonka pituus on 17 merkkiä, tunnistetaan osapuolet. Pankin tunnuksena on yleensä pankin LY-tunnus. Pankki antaa asiakkaalle asiakkaan käyttämän tunnuksen, ns. PATU-asiakastunnuksen. Kentän pituus sallii OVT-tunnusstandardin SFS 5748 mukaisen tunnuksen käytön. Tunnuksen käyttö kuvataan kunkin pankin omassa järjestelmäkuvauksessa.

Pankki käyttää tarkennekenttää, jonka pituus on 8 merkkiä, eri tarkoituksiin, kuten esimerkiksi tunnistamaan asiakasyrityksen eri järjestelmiä tai eri tarkoituksiin käytettäviä salaisia avaimia. Ellei tarkennetta käytetä, kenttä täytetään tyhjämärkeillä.

3.1.3 Asiakasjärjestelmien työnkulku

Turvasanomiam käsittelevät työvaiheet voidaan toteuttaa eri tavoin ja suorittaa erillisessä turvatuss ympäristössä sekä aineistoerän luonnista että lähetyksestä erillään. Kuvauksessa esitettävät menetelmät mahdollistavat turvasanomien muodostamisen aineistoerän luontivaiheessa, erillisessä työvaiheessa tai tiedonsiirron yhteydessä.

Yhteydellisessä tiedostosiirrossa pankkien järjestelmät tarkastavat todentamis- ja suojaustiedot siirron aikana. Pankin asiakkaalle lähettämät turvasanomiat voidaan tarkastaa tiedonsiirron yhteydessä tai myöhemmin. Suositeltavaa on, että asiakas tarkastaa esittäytymissanomat heti yhteyden aikana

Turvamenetelmän käyttöönoton yhteydessä asiakasjärjestelmän on varauduttava käsittelemään pankin järjestelmän antamia uusia, tässä dokumentissa mainitsemattomia virheilmoituksia.

3.1.4 Tietoturva vaatimukset

Pankki ja asiakas sopivat siitä, mitkä aineistotyypit suojataan. Suojauksen käyttö alkaa pankin ja asiakkaan välisessä sopimuksessa sovittuna päivänä ja suojauksen käyttö on siitä alkaen pakollista kaikille sovituille aineistotyypeille.

Pankin ja asiakkaan tietojärjestelmissä on tallettuna tieto siitä, mitkä tunnukset (TUNNUS ja TARKENNE) ovat asiakkaan käytössä.

Asiakas säilyttää aineistotyyppi- ja pankkikohtaisesti tiedon siitä, käytetäänkö aineiston suojausta. Pankki säilyttää vastaavat tiedot. Aineistotyyppien yhteydessä luetellaan tunnukset (TUNNUS ja TARKENNE), joita voidaan käyttää ko. aineistoerien suojaamiseen. Kun pankkiin lähtevälle aineistotyyppille käytetään aineiston suojausta, käytetään aina myös aineistoerän vastaanoton varmistamista.

3.1.5 Turvasanomiat

PATU-turvamenettelyn yhteydessä käytettävät sanomatyyppikoodit ja sanomat ovat:

- ESI, esittäytymissanoma
- SUO, suojausotsake
- VAR, suojauslopuke
- PTE, palautesanoma

Turvasanomien rakenne on kiinteä, ja eri sanomatyyppien tietosisältö on samankaltainen. Sanoma



koostuu yhteisestä alkuosasta ja sanomatyyppikohtaisesta lisäosasta.

ESI-, VAR- ja PTE-sanomia käytetään lisäksi avainjakeluun.

ESI

ESI-sanomaa käytetään asiakkaan ja pankin todentamisessa.

SUO, VAR

Suojattu aineistoerä välitetään suojauskehyksessä, joka koostuu aineistoerää edeltävästä SUO-sanomasta ja aineistoerän jäljessä olevasta VAR-sanomasta.

PTE

Pankki varmistaa aineistoerän vastaanoton lähettämällä asiakkaalle PTE -sanoman, joka korvaa aiemmin käytetyt koontisummasanomat. Sanoma voi sisältää pankkikohtaiset aineistoerän kuittauksetiedot.

Asiakas ei anna pankille PTE -kuittauksta vastaanottamistaan aineistoerästä.

3.2 Pankin ja asiakkaan todentaminen

Yhteydellisessä tiedostosiirrossa esittäytyminen ja todentaminen suoritetaan yhteyden muodostamisen alussa. Asiakas lähettää pankille ESI-sanomansa ja pankki vastaa asiakkaalle omalla ESI-sanomallaan. Yhteydettömässä tiedostosiirrossa esittäytyminen hoidetaan asiakkaan tai pankin lähettämän tiedoston alussa olevalla ESI-tietueella.

Osapuolet todentavat toisensa tarkastamalla vastapuolen lähettämän ESI-sanoman. Sanomassa on MAC-menetelmällä laskettu tarkiste, jonka avulla vastaanottaja todentaa lähettäjän. Tarkiste lasketaan turvasanoman ensimmäisestä merkistä tarkistetta edeltävään merkkiin käyttäen asiakas- ja pankkikohtaisia salaista avainta.

ESI-sanoma sisältää aikaleiman. Samaa aikaleimaa ei saa käyttää kahdesti. Asiakas muodostaa aikaleiman ja pankki tarkastaa sen ainutkertaisuuden vertaamalla sitä asiakkaan aikaisemmin käyttämiin aikaleimoihin. Aikaleiman päivämäärä saa olla korkeintaan viisi pankkipäivää vanha. Vastauksena lähettä-

mässä ESI-sanomassa pankki käyttää asiakkaan ESI-sanomassa ollutta aikaleimaa. Asiakas tarkastaa, että vastaanotetun sanoman aikaleima on sama kuin lähetetyn sanoman aikaleima.

3.3 Siirto- ja aineistoerän suojaaminen

Aineisto voidaan suojata joko siirtoerä- tai aineistoeräkohtaisesti (kts. 3.5.3) Suojattava siirtoerä koostuu yhdestä tai useammasta aineistoerästä.

Suojattava erä sijoitetaan turvakehykseen. Erän eteen sijoitetaan suojausotsake eli SUO-sanoma ja aineiston perään suojauslopuke eli VAR-sanoma.

Erän suojaus tehdään kahdessa vaiheessa. Ensimmäisessä erästä lasketaan tiiviste, joka sijoitetaan VAR-sanomaan. Sitten VAR-sanomasta lasketaan tarkiste, joka liitetään samaiseen VAR-sanomaan.

Tiivistelaskennassa käytettävä avain muodostetaan jokaista käyttöä varten erikseen ja on sisällöltään satunnainen. Avainta kutsutaan kerta-avaimeksi. Kerta-avain välitetään siirto- tai aineistoerän mukana SUO- ja VAR-sanomissa salakirjoitettuna.

VAR-sanoman tarkisteen laskenta tehdään samalla tavalla kuin ESI-sanoman kohdalla. Suojatun erän lähettäjä generoi joka erälle aikaleiman, joka sijoitetaan SUO- ja VAR-sanomiin. Pankki tarkastaa vastaanottamiensa aikaleimojen ainutkertaisuuden vertaamalla aikaleimaa asiakkaan aikaisemmin käyttämiin aikaleimoihin. Asiakas voi suorittaa saman tarkastuksen pankin lähettämille aikaleimoille.

3.4 Suojatun erän vastaanoton varmistaminen

Pankki kuittaa vastaanottamansa suojatun erän lähettämällä PTE-sanoman, jonka avulla asiakas voi varmistua erän perillemenosta. Sanoma sisältää saman aikaleiman, kerta-avaimen ja tiivisteen, jotka olivat asiakkaan lähettämän erän VAR-sanomassa. Pankki laskee sanomaan tarkisteen pankin ja asiakkaan yhteisellä salaisella avaimella.

3.5 Välittäjän ja omistajan tekemät suojaukset

3.5.1 Palveluverkon ja palvelukeskuksen rooli

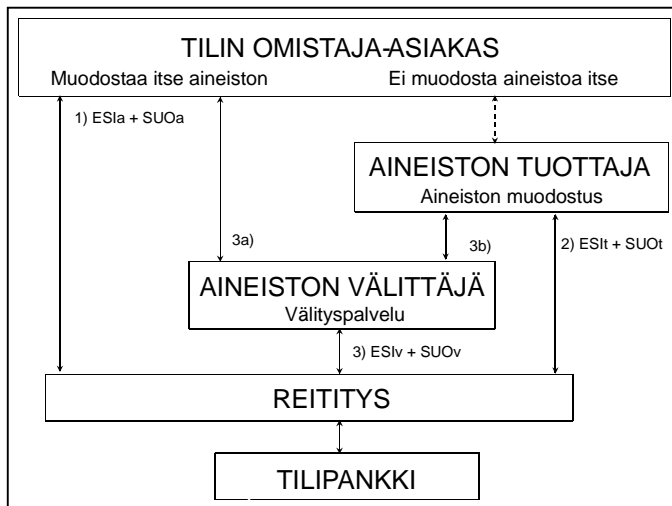
Asiakas voi lähettää tai saada toimittaa muodostamansa aineiston tilipankkiin suoraan tai välittäjänä toimivan palvelutalon tai palveluverkkojen kautta. Asiakas voi käyttää palvelutaltoa aineistonsa tuot-



tajana, joka voi välittää aineiston tilipankin suoraan tai palvelutalon kautta. Asiakasta, jonka aineistoerästä on kyse, sanotaan **omistaja-asiakkaaksi**, ja palvelukeskusta tai palveluverkkoa sanotaan **välittäjäasiakkaaksi**. Välittäjäasiakas voi:

- 1) tuottaa tai käsitellä aineistoerän omistaja-asiakkaan puolesta, ns. *aineiston tuottaja*, esimerkiksi ajamalla palkkasovellusta).
- 2) välittää, esim. palveluverkon välivaraston kautta, omistaja-asiakkaan aineistoerän pankkiin sellaisenaan tai pienillä muutoksilla, ns. *aineiston välittäjä*. Pieniä muunnoksia voivat olla
 - koodikonversio (esim. ASCII -> EBCDIC)
 - muunto vaihtuvanmittaisten ja kiinteänmittaisten tietue- tai sanomamuotojen välillä
 - aineistoerän jaksottaminen ja jakaminen
- 3) tehdä esitystapamuunnoksia omistaja-asiakkaan aineistoerälle pankin ja asiakkaan käyttämien esitystapojen välillä, ns. *aineiston välittäjä*. Esitystapamuunnos voi olla esimerkiksi EDIFACT-muunnos).

PATU -menettelyn suojaus ei ulotu kohdassa 3 mainittujen aineistonrakennetta muuttavien esitystapamuunnosten yli.



Kuva 1. Aineistojen muodostus ja välitysreitit

3.5.2 Aineiston suojaus

Peruseriaatteena on, että aineistoerän suojauksen laskee osapuoli, joka tuottaa aineistoerän pankkien palvelukuvausten mukaiseen muotoon.

Aineistot suojataan mahdollisimman varhaisessa vaiheessa. Suositellaan, että SUO/VAR- ja ESI-

sanomat lasketaan aina yhdessä pisteessä. Ellei aineiston muodostaja suoja aineistoja, niin aineiston välittäjänä oleva osapuoli laskee kullekin siirtoerälle Patu-suojauksen omilla avaimillaan. Omistaja-asiakas tai aineiston tuottaja eivät laske SUO/VAR-sanomia kuvan 1 vaihtoehdoissa 3a) eikä 3b), vaan suojauksen tekee aineiston välittäjä.

Suojausta ei tehdä kahteen kertaan eli yhteen aineistoerään ei voi liittyä sekä omistajan että välittäjän suojausta.

3.5.3 Suojauksessa käytettävä avain

Suojauskehyksessä, eli suojattua aineistoerää edeltävässä SUO-sanomassa ja jäljessä seuraavassa VAR-sanomassa, kentän LÄHETTÄJÄ sisältämä asiakkaan tunnus ilmoittaa kenen avaimilla erän suojaus on laskettu.

Pankki sopii asiakkaan kanssa sopimuksen teon yhteydessä pankista noudettavien aineistojen osalta aineistokohtaisesti erikseen, kenen (omistaja/välittäjä-asiakas) avaimia aineistojen suojaukseen käytetään. Pankki ilmoittaa SUO-sanomassa olevalla asiakastunnuksella kenen avainta se on käyttänyt aineiston suojauksessa.

3.5.4 Suojattava kokonaisuus

A. Yhteydellinen tiedostosiirto

Yhteydellisessä tiedostosiirrossa siirtoerä alkaa sovellussanomien jälkeen ja loppuu seuraavaan ohjussanomaan. Siirtoerään voi sisältyä yksi tai useampia aineistoeriä.

Yhteydellisen tiedostosiirron siirtoerä suojataan yhtenä kokonaisuutena. Tarvittaessa muodostetaan useampia siirtoeriä.

Pankin antamaa palautteena yhden PTE-sanoman kutakin suojattua siirtoerää kohti. PTE-sanoma sisältää aina siirtoerän kuittautiedot. Se korvaa aiemmin käytössä olleen koontisummasanomien.

B. Yhteydetön tiedostosiirto

Yhteydettömässä tiedostosiirrossa siirtoerä on tiedosto, joka sisältää yhden tai useampia aineistoeriä. OVT-kuljetusmenettelyä käytettäessä siirtoerää edeltää kuljetuskehyksen alkumerkintä ja sitä seuraa loppumerkintä.



Yhteydettömän tiedostosiirron siirtoerä voidaan suojata joko yhtenä kokonaisuutena tai sen sisältämät aineistoerät voidaan suojata kukin erikseen. Siirtoerässä voi olla suojattuja ja suojaamattomia aineistoeriä, kun käytetään aineistoeräkohtaista suojausta.

Pankin antamassa palautteessa on yksi PTE-tietue jokaista suojattua erää kohden. PTE-tietueet esiintyvät samassa järjestyksessä kuin vastaavat suojatut erät alkuperäisessä tiedostossa.

OVT-kuljetuskehystä käytettäessä PTE-tietueet si-
joitetaan kuittauskehykseen mahdollisten aineisto-
eriä koskevien vapaamuotoisten tietueiden yhtey-
teen.

3.5.5 Sopimukset

Peruseriaatteenä on, että pankkiin tietoyhteydessä olevalla osapuolella tulee olla siihen oikeuttava sopimus pankin kanssa. Pankkien sopimusten rakenne eroavat toisistaan, mutta yhteisenä piirteenä on se, että tiliasiakkaan ja pankin välisiin sopimuksiin rekisteröidään aineistotyytit ja niiden välittäjät.

Pankki edellyttää, että aineistot suojataan aina tiliasiakkaan sopimuksessa sovitun osapuolen avaimilla. Esittäytyminen voi tapahtua palvelutalon omilla tunnuksilla ja avaimilla

Tiliasiakas ja aineiston tuottaja sopivat keskenään aineiston tuottamiseen liittyvistä palveluista. Samalla aineiston tuottaja antaa tiliasiakkaalle aineiston välittäjänä toimivan organisaation tiedot.

Tiliasiakas tekee itse sopimuksen pankkinsa kanssa tai valtuuttaa tuottajan palvelutalon tekemään sopimuksen puolestaan. Suositellaan, että tiliasiakas tekee itse sopimuksen pankkinsa kanssa. Sopimuksessa sovitaan maksuliikenneaineistojen välittämiseen liittyvät asiat ja aineiston välittäjäksi merkitään tuottajan tiliasiakkaalle antaman ohjeen mukainen välittäjä.

Välittäjä voi olla joko tuottaja tai kolmas osapuoli, jonka kanssa tuottaja on sopinut aineistojensa välittämisestä.

Osalla pankeista on erilliset sopimukset välitettävistä aineistoista ja tietoliikenne-käytännöistä. Osa ns. peruspalveluihin liittyvistä asioista on saatettu yhdistää tietoliikenneasioiden kanssa samaan sopimukseen. Näiden sopimusten lisäksi pankeilla on

erilliset sopimukset maksupääte- ja maksukorttiai-
neistojen välitystä varten.



4 TURVASANOMAT JA NIIDEN KÄYTTÖ

4.1 Turvasanomien tiedot

Aakkosnumeeriselle kentälle tieto sijoitetaan kenttään vasemmalta alkaen ja kentän loppuosa täytetään tyhjämerkeillä, numeeriselle kentälle tieto sijoitetaan kenttään oikealle tasattuna ja kentän alku täytetään etunollilla.

Kun tietoa ei käytetä sanomassa, kentässä on oltava tyhjämerkkejä (aakkosnumeeriset tiedot) tai nollia (numeeriset tiedot).

Pankki pyrkii antamaan oman tunnuksensa ja asiakastunnuksen OVT-tunnusstandardin SFS 5748 mukaisena.

Turvasanomista käytetään seuraavia lyhenteitä:

- ESla asiakkaan lähettämä ESI-sanoma
- ESlp pankin lähettämä ESI-sanoma

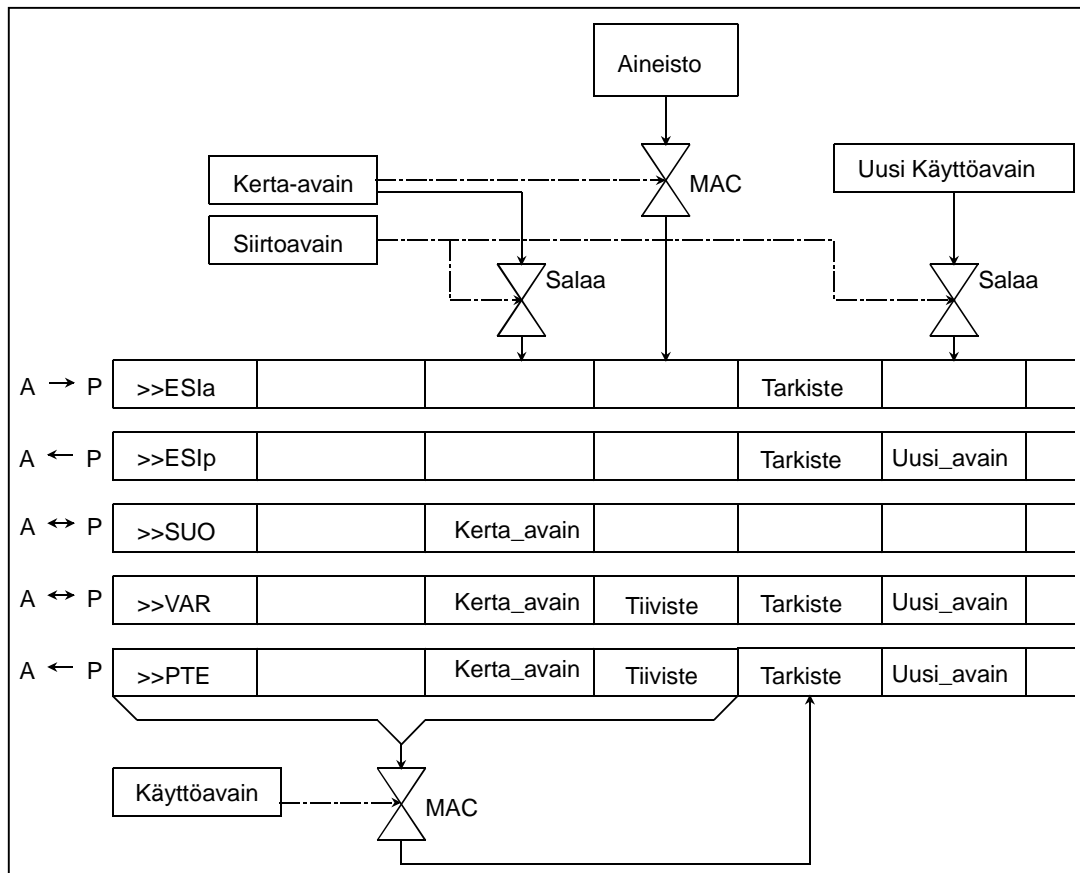
- SUOa asiakkaan lähettämä SUO-sanoma
- SUOp pankin lähettämä SUO-sanoma
- VARa asiakkaan lähettämä VAR-sanoma
- VARp pankin lähettämä VAR-sanoma
- PTE pankin lähettämä palautesanoma

Turvasanomien tiedot on esitetty liitteessä 1.

4.2 Tietojen käyttö eri turvasanomissa

Avainkentät, tarkistuskentät ja niiden käyttö ilmenevät oheisesta kuvasta 2. Kerta-avain ja uusi käyttöavain esiintyvät turvasanomissa siirtoavaimella salakirjoitettuina. Tiivisteen laskennassa käytetään kertaavainta ja tarkisteen laskennassa käyttöavainta.

Eri turvasanomissa käytettävät tiedot on kuvattu liitteessä 2.



Kuva 2. Turvasanomien muodostus



4.3 Pankin ja asiakkaan todentaminen

ohjeet sisältyvät kunkin pankin järjestelmäkuvaukseen.

4.3.1 Esittäytyminen yhteydellisessä tiedostosiirrossa

Asiakkaan tulee tarkastaa pankin lähettämä ESIP-sanoma yhteyden aikana ennen aineistojen siirtoa.

Yhteydenotto pankin järjestelmään tehdään pankki-kohtaisten menetelmien mukaan. Yksityiskohtaiset

| ASIAKAS | SANOMA | PANKKI |
|---|---|---|
| 1. Muodostetaan ja lasketaan ESISanoma valmiiksi | | |
| 2. Muodostetaan yhteys | -----> | Yhteys muodostunut |
| 3. Lähetetään sanoma | --- >>ESIA.... ---> | Vastaanotto ja tarkastus, vastauksen muodostaminen |
| 4. Vastauksen tarkastus ja talletus | <--- >>ESIP.... ----- jatketaan tiedostosiirrolla..... | Vastauksen lähetys |
| 5. Katkaistaan yhteys | | |
| 6. Tarkastetaan talletettu vastaus: mm. sisältääkö sanoma uuden avaimen | | |

Esimerkki 1. Yhteydenotto pankkiin yhteydellisessä tiedostosiirrossa.

4.3.2 Esittäytyminen yhteydettömässä tiedostosiirrossa

Esimerkki 2 kuvaa yhteydettömässä tiedostosiirrossa tapahtuvaa molemminpuolista esittäytymistä. Asiakas ja pankki lisäävät ESI-tietueita välitettäviin tiedostoihin. Asiakkaan lähettämä tiedosto on seuraavanlainen:

```
'''ED2 aineistokehys.....
>>ESIA .....
..dataa.....
..dataa.....
'''EOF aineistokehys.....
```

Esimerkki 2a. Asiakkaan lähettämä tiedosto

Pankki antaa kuittauksen seuraavanlaisena tiedostona:

```
'''CON kuittauskehys.....
>>ESIP .....
..kuittautustietueet.....
'''EOF kuittauskehys.....
```

Esimerkki 2b. Pankin antama kuittautiedosto

Tiedon kuljetus tehdään asiakkaan ja pankin sopimilla tavoilla. Esimerkissä oletetaan noudatettavan OVT-kuljetusmenettelyä. Ellei sitä noudateta, kehys- ja kuittautustietueet puuttuvat tai ovat erilaisia.

4.3.3 Pankin suorittamat tarkastukset

Todentamiseen liittyvät seuraavat tarkastukset (suluissa on mainittu kyseeseen tulevat kohdassa 7 selostetut ilmoituskoodit):

- 1) Pankki tarkastaa omasta tietokannastaan onko asiakkaan kanssa sovittu todennuksen käytöstä. Jos on, esittäytyminen täytyy tehdä ESIA-sanomassa / tiedostossa on oltava ESIA-tietue.
- 2) Tarkastetaan ESIA-sanoman muoto ja tietojen oikeellisuus (1010 - 1011).
- 3) Tarkastetaan, onko VERSIO niin vanha, ettei sitä enää tueta (1012).
- 4) Vastaanottajan tunnuksen (VASTAANOTTAJA) täytyy olla oma tunnus (1021).
- 5) Aikaleiman PÄIVÄYS saa olla korkeintaan viisi pankkipäivää vanha (1015), eikä se saa viitata tulevaisuuteen (1016).
- 6) AIKALEIMA ei saa olla kopio aikaisemmin käytetystä aikaleimasta (1018).
- 7) Siirto- ja käyttöavaimien sukupolvinumeroina on oltava nykyisten avaimien sukupolvinumerot. Kun aikaleiman päiväys on vaihtojakson päivämäärien välissä, sukupolvinumerona saa olla myös edellisen avaimen sukupolvinumero (1013, 1014).



- 8) Pankki laskee tarkisteen ja tarkastaa, että TARKISTE-kentässä oleva arvo on sama (1020).
- 9) Ellei virhettä löydy, todennus hyväksytään ja aikaleima merkitään käytetyksi (ONNISTUMIS-KOODIn arvona palautetaan K). Pankki tarkastaa voiko se hyväksyä pyydetyn käyttöavaimen vaihdon (1002 - 1005) tai vaihtojakson katkaisun (1036 - 1037).

Jos tarkastuksessa löytyy virhe, pankki kirjoittaa ilmoituksen lokiin ja ilmoittaa ESIP-sanomassa/tietueessa virheestä asiakkaalle. Tarkastusten 1 - 8 tapauksessa pankki katkaisee yhteyden ja hylkää tiedoston (ONNISTUMISKOODIn arvona palautetaan E)

4.3.4 Asiakkaan suorittamat tarkastukset

Todentamiseen liittyvät seuraavat tarkastukset (suluissa on mainittu kyseeseen tulevat kohdassa 7 selostetut ilmoituskoodit):

- 1) Asiakas tarkastaa omasta tietokannastaan, onko pankin kanssa sovittu todennuksen käytöstä. Jos on, esittäytyminen täytyy tehdä ESIP-sanomassa / -tiedostossa on oltava ESIP-tietue.
- 2) Asiakas tarkastaa ESIP-sanoman muodon ja tietojen oikeellisuuden (3010 - 3011).
- 3) Vastaanottajan tunnuksen (VASTAANOTTAJA) täytyy olla asiakkaan oma tunnus (3021).
- 4) AIKALEIMAN tulee olla sama kuin vastaavassa ESIA-sanomassa/ESIA-tietueessa (3022).

- 5) Siirto- ja käyttöavainten sukupolvinumeroiden pitää olla samat kuin ESIA-sanomassa (3011)
- 6) Asiakas laskee tarkisteen ja tarkastaa, että TARKISTE-kentässä oleva arvo on sama (3020).
- 7) Jos AVAINVAIHTO on 1, tarkastetaan uuden käyttöavaimen pariteetti (3030).
- 8) Asiakas tarkastaa pankin antamat ilmoituskoodit.

Jos tarkastuksessa löytyy virhe, asiakas kirjoittaa ilmoituksen lokiin ja soittaa pankin yhteyshenkilölle sekä katkaisee siirtoyhteyden ja hylkää tiedoston.

4.4 Aineistoerien suojaaminen

Suojauksen tarkoituksena on varmistaa sekä pankille että asiakkaalle tiedon muuttumattomuus. Suojaus toteutetaan suojausotsakkeen (SUO-sanoma), suojausloputteen (VAR-sanoma) ja palautesanomien (PTE-sanoma) avulla.

4.4.1 Aineistoerien suojaaminen yhteydellisessä tiedostosiirrosta

Esimerkit 3 ja 4 kuvaavat suojatun tiedon lähettämistä ja hakemista yhteydellisessä tiedostosiirrosta. Esimerkit kuvaavat yhteyttä, jossa käytetään sekä EOF- että nk. hyväksymis-/hylkäyssanomaa. Tapauksissa, joissa pankkiyhteydellä ei ko. sanomia ole käytössä, esimerkki on samanlainen lukuunottamatta puuttuvia EOF- ja HYV-sanomia. Asiakkaan tulisi tarkastaa ESI-turvasanomien yhteydenoton aikana.

| ASIAKAS | SANOMA | PANKKI |
|---|-----------------------------|------------------------------------|
| Aineistoerä on muodostettu ja se sisältää SUO- ja VAR-sanomat | | |
| 1. Yhteyden muodostus ja esittäytyminen | ---- >>ESIA..... ----> | Tarkastus ja vastauksen lähetykset |
| 2. ESIP:n tarkastus ja talletus | <---- >>ESIP..... ----> | Tarkastus ym. |
| 3. Sovellustiedon lähetykset | ---- //sov,era ----> | Tarkastus |
| 4. Datatien lähetykset | ---- >>SUOA..... ----> | |
| | ---- .dataa..... ----> | |
| | ---- >>VARa..... ----> | Tarkastus |
| 5. (EOF-sanoman lähetykset) | ---- ...EOF..... ----> | |
| 6. Palautevastaanotto ja talletus | <---- >>PTEp....KOONTI. --- | Palautevastaanotto ja lähetykset |
| 7. (HYV-lähetykset) | ---- ...HYV..... ----> | Eräillä pankeilla käytössä |
| muita aineistoerien lähetyksiä ja hakuja | | |
| 8. Katkaistaan yhteys | | |
| 9. Tarkastetaan talletetut ESIP- ja PTE-sanomat | | |

Esimerkki 3. Aineistoerän lähetykset pankkiin vuorovaikutteisessa tiedonsiirrosta



| ASIAKAS | SANOMA | PANKKI |
|--|------------------------|----------------------|
| 1. Yhteyden muodostus ja esittäytyminen | ---- >>ESla..... ----> | Tarkastus ja vastaus |
| 2. ESIp:n tarkastus ja talletus | <---- >>ESIp..... ---- | Tarkastus ym. |
| 3. Hakupyynnön lähetys | ---- //sov,era ----> | Datan lähetys |
| 4. Datan vastaanotto | <---- >>SUOp..... ---- | |
| | <---- .dataa..... ---- | |
| 5. (Vastaanotto | <---- >>VARp..... ---- | EOF:in lähetys) |
| 6. SUOp- ja VARp-sanomien talletus | <---- ...EOF..... ---- | |
| muita aineistoerien lähetyksiä ja hakuja | | |
| 7. Katkaistaan yhteys | | |
| 8. Lasketaan aineistoerän tiiviste | | |
| 9. Tarkastetaan talletetut ESIp-, SUOp- ja VARp-sanomat | | |

Esimerkki 4. Aineistoerän haku pankista vuorovaikutteisessa tiedonsiirrossa

4.4.2 Aineistoerien suojaaminen yhteydettömässä tiedostosiirrossa

Suojaustietueiden (ESI, SUO, VAR ja PTE) sijainti on määritelty Suomen Pankkiyhdistyksen kuvauksessa "Pankkien asiakasliittymäkuvaus, yhteydetön tiedostosiirto", TSJ 93001.

Asiakas ja pankki lisäävät aineistoeriin suojauskehukset, SUO-tietueen ennen aineistoerää ja VAR-tietueen aineistoerän perään. Esimerkeissä 5a ja 5b olevien OVT-kuljetusmenettelyjen käyttö on pankki-kohtaista ja voi puuttua kokonaan.

Yhteydettömässä tiedonsiirrossa asiakkaan lähettämä tiedosto on:

```
'''ED2 aineistokehys.....
>>ESI.....
>>SUO.....
..dataa, aineistoerä 1....
>>VAR.....
>>SUO.....
..dataa, aineistoerä 2....
>>VAR.....
'''EOF aineistokehys.....
```

Esimerkki 5a. Asiakkaan lähettämä tiedosto

Palaute esimerkin 5a tiedostoon on:

```
'''CON kuittauskehys.....
>>ESI.....
..OVT-kuittaus, ain.erä 1..
>>PTE.....
..OVT-kuittaus, ain.erä 2..
>>PTE.....
'''EOF kuittauskehys.....
```

Esimerkki 5b. Palaute esimerkin 5a sanomiin.

Jos lähetys sisältää useita erikseen suojattuja aineistoeria, on kuittauksessa vastaavasti useita PTE-tietueita.

4.4.3 Pankin tarkastukset SUO- ja VAR-sanomille

Suojaukseen liittyvät seuraavat tarkastukset (suluissa on mainittu kyseeseen tulevat kohdassa 7 selostetut ilmoituskoodit):

- 1) Pankki tarkastaa tietokannastaan, onko asiakkaan kanssa sovittu suojauskehyksen käytöstä tämän aineistotyypin kohdalla. Aineistoerää pitää edeltää SUO-sanoma ja seurata VAR-sanoma, jos suojauskehyksen käytöstä on sovittu.
- 2) Tarkastetaan turvasanomien muoto ja tietojen oikeellisuus (1010, 1011).
- 3) Tarkastetaan, onko VERSIO niin vanha, ettei sitä enää tueta (1012).
- 4) Vastaanottajan tunnuksen (VASTAANOTTAJA) täytyy olla oma tunnus (1021).
- 5) Asiakkaalla (LÄHETTÄJÄ) täytyy olla oikeus suojata tämä aineistotyyppi (1025).
- 6) SUO- ja VAR-sanomissa seuraavilla kentillä pitää olla samat arvot (1026):
 - VERSIO,
 - VASTAANOTTAJA,
 - LÄHETTÄJÄ,
 - KERTAAVAIN,
 - SIIRTOAVAINNO,
 - KÄYTTÖAVAINNO,
 - SUOJAUSALUE ja



- AIKALEIMA
- 7) Aikaleiman PÄIVÄYS saa olla korkeintaan viisi pankkipäivää vanha (1015), eikä se saa viitata tulevaisuuteen (1016).
- 8) AIKALEIMA ei saa olla kopio aikaisemmin käytetystä aikaleimasta (1018).
- 9) Siirto- ja käyttöavaimien sukupolvinumeroina on oltava nykyisten avaimen sukupolvinumerot. Kun aikaleiman päiväys on vaihtojakson päivämäärin välissä, sukupolvinumerona voi olla myös edellisen avaimen sukupolvinumero (1013, 1014).
- 10) SUO-sanoman kerta-avaimen pitää olla ainutkertainen (1017) ja pariteetin pariton (1031).
- 11) Pankki laskee aineistoerän tiivisteeseen ja tarkastaa, että TIIVISTE-kentässä oleva arvo on sama (1019).
- 12) Pankki laskee VAR-sanoman tarkisteen ja tarkastaa, että TARKISTE-kentässä oleva arvo on sama (1020).
- 13) Ellei SUO- ja VAR-sanomien tarkastuksessa löydy virhettä, suojaus hyväksytään ja aikaleima sekä kerta-avain merkitään käytetyksi, (ONNISTUMISKOODIn arvona palautetaan K).
- 14) Pankki tarkastaa voiko se hyväksyä pyydetyn käyttöavaimen vaihdon (1002 - 1005) tai käyttöavaimen vaihtojakson katkaisun (1036 - 1037).

Jos tarkastuksessa löytyy virhe, pankki kirjoittaa ilmoituksen lokiin ja ilmoittaa PTE-sanomassa / tietueessa virheestä asiakkaalle. Tarkastusten 1 - 12 tapauksessa pankki hylkää aineistoerän (ONNISTUMISKOODIn arvona palautetaan E).

4.4.4 Asiakkaan tarkastukset PTE-sanomalle

PTE-sanomaan / tietueeseen liittyvät seuraavat tarkastukset (suluissa on mainittu kyseeseen tulevat kohdassa 7 selostetut ilmoituskoodit):

- 1) Asiakas tarkastaa tietokannastaan, onko pankin kanssa sovittu suojausten käytöstä tämän aineistotyyppin kohdalla. Jos on, niin pankille lähetettävään aineistoeraan on tultava palautteena PTE-sanoma pankilta (3029)
- 2) Tarkastetaan turvasanomien muoto ja tietojen oikeellisuus (3010 - 3011).

- 3) Vastaanottajan tunnuksen (VASTAANOTTAJA) täytyy olla oma tunnus (3021).
- 4) Asiakkaan SUO- ja vastaavassa pankin PTE-sanomassa seuraavilla kentillä pitää olla vastaavat arvot (3027):
 - VASTAANOTTAJA,
 - LÄHETTÄJÄ,
 - AIKALEIMA,
 - SUOJAUSALUE ja
 - KERTA-AVAIN.
- 5) Asiakkaan VAR- ja vastaavassa pankin PTE-sanomassa TIIVISTE-kentässä pitää olla samat arvot (3028).
- 6) Siirto- ja käyttöavainten sukupolvinumeroiden pitää olla samat kuin VARa-sanomassa (3011)
- 7) Asiakas laskee tarkisteen ja tarkastaa, että TARKISTE-kentässä oleva arvo on sama (3020).
- 8) Jos AVAINVAIHTO on 1, tarkastetaan uuden käyttöavaimen pariteetti (3030). Asiakas tarkastaa pankin antamat ilmoituskoodit.

Jos tarkastuksessa löytyy virhe, asiakas kirjoittaa ilmoituksen lokiin ja ottaa yhteyden pankin yhteyshenkilöön.

4.4.5 Asiakkaan tarkastukset SUO- ja VAR-sanomille

SUO- ja VAR-sanomaan / tietueeseen liittyvät seuraavat tarkastukset (suluissa on mainittu kyseeseen tulevat kohdassa 7 selostetut ilmoituskoodit):

- 1) Asiakas tarkastaa omasta tietokannastaan onko pankin kanssa sovittu suojausten käytöstä tämän aineistotyyppin kohdalla. Jos on, niin aineistoerää pitää edeltää SUO-sanoma ja seurata VAR-sanoma (3023, 3024)
- 2) Tarkastetaan turvasanomien muoto ja tietojen oikeellisuus (3010 - 3011).
- 3) Vastaanottajan tunnuksen (VASTAANOTTAJA) täytyy olla oma tunnus (3021).
- 4) Pankilla (LÄHETTÄJÄ) täytyy olla oikeus suojata tämä aineistotyyppi - ei välttämätön tarkastus (3025).



- 5) SUO- ja VAR-sanomien seuraavissa kentissä pitää olla samat arvot (3026):
- VERSIO
 - VASTAANOTTAJA
 - LÄHETTÄJÄ
 - KERTAAVAIN
 - SIIRTOAVAINNO
 - KÄYTTÖAVAINNO
 - SUOJAUSALUE
 - AIKALEIMA.
- 6) AIKALEIMAN PÄIVÄYS saa olla korkeintaan viisi pankkipäivää vanha (3015) eikä se saa viitata tulevaisuuteen (3016).
- 7) AIKALEIMA ei saa olla kopio aikaisemmin käytetystä aikaleimasta (3018).
- 8) Siirto- ja käyttöavaimien sukupolvinumeroina on oltava nykyisten avaimen sukupolvinumerot. Kun aikaleiman päiväys on vaihtojakson päivämäärin välissä, sukupolvinumerona saa olla myös edellisen avaimen sukupolvinumero (3013, 3014).
- 9) SUO-sanoman kerta-avaimen pitää olla ainutkertainen (3017) ja pariteetin pariton (3031). Ainutkertaisuuden tarkastaminen ei ole välttämätöntä.
- 10) Asiakas laskee aineistoerän tiivisteen ja tarkastaa, että TIIVISTE-kentässä oleva arvo on sama (3019).
- 11) Asiakas laskee VAR-sanomalle tarkasteen ja tarkastaa, että TARKISTE-kentässä oleva arvo on sama (3020).
- 12) Aikaleima merkitään käytetyksi, ellei tarkastuksissa havaita virhettä
- 13) Jos VAR-sanomassa AVAINVAIHTO-kentän arvo on 1, tarkastetaan uuden käyttöavaimen pariteetti (3030).

Jos tarkastuksessa löytyy virhe, asiakas kirjoittaa ilmoituksen lokiin, hylkää aineistoerän ja ilmoittaa virheestä pankin yhteyshenkilölle

4.5 Turvasanomien jakomenettely

PATU-menettelyissä käytettävät turvasanomien ovat yli 80 merkkiä pitkiä ja on odotettavissa, että niiden pituus kasvaa muutosten yhteydessä. Sanomien maksimipituus on 500 merkkiä. Muutosjoustavuuden

säilyttämiseksi on tärkeää, että alla olevia sääntöjä noudatetaan niiden käsittelyssä.

Turvasanomien jakomenettely tarvitaan silloin, kun jokin järjestelmä asettaa ylärajan sanomapituudelle. Tietoliikenteessä raja saattaa olla 80 merkkiä. Tietovälineillä käytetään usein kiinteää tietuepituutta. Tällöin raja riippuu aineistotyyppistä ja voi olla esim 80, 90 tai 300 merkkiä.

Jakosäännöt koskevat yhtäläillä tietoliikenneyhteyttä kuin tiedosto-välitystä, joten "sanoman" tilalla voi yhtä hyvin olla "tietue".

4.5.1 Käsittelysäännöt

a) Fyysinen sanoma sama kuin looginen sanoma

Suosittelaa, että fyysinen sanoma on sama kuin looginen sanoma.

Vastaanottaja varautuu 500 merkin mittaisiin sanomiin, mutta käsittelee ne sanomaan sisältyvän sanomapituuden ja versionumeron mukaan. Lähettäjä lähettää loogisen sanoman käyttämänsä PATUn version sanomakuvausten pituisena.

b) Fyysinen sanoma pitempi kuin looginen sanoma

Loogisen sanoman alku sijoitetaan aina fyysisen sanoman alkuun ja fyysisen sanoman loppupää täytetään tyhjämerkeillä, jos fyysinen sanoma on pidempi kuin looginen sanoma.

c) Fyysinen sanoma lyhyempi kuin looginen sanoma

Sanoma jaetaan fyysisen sanoman pituisiin osiin (välittämättä tietojen rajoista) ja siirretään tarpeellisen monena fyysisenä sanomana, jos looginen sanoma on pitempi kuin fyysisen sanoman maksimipituus.

Jos viimeinen osa on lyhyempi kuin fyysisen sanoman maksimipituus, sen voi lähettää joko niin, että fyysinen sanoma on yhtä pitkä kuin osa tai fyysinen sanoma täytetään tyhjämerkeillä maksimipituuteensa.

Vastaanottaja lukee niin monta fyysistä sanomaa, että loogisen sanoman sanomapituuskentän mukainen pituus tulee täyteen. Ohjelman tekohelellä voimassaolevaa sanomapituutta ei pidä käyttää tähän, se voi aiheuttaa virheellistä toimintaa turvasanomien pituuksien muuttuessa.



Ohjelmoitaessa turvasanomien vastaanotossa on huomioitava, että sanomien pituus voi kasvaa PATU-määrityksen muutosten takia. Sanomassa on silloin uusi sanomapituus-tieto, joka on suurempi kuin vanhassa sanomassa. Vanhan sanoman kentät ja tiedot pysyvät entisillä paikoillaan ja niitä käytetään kuten ennenkin. Fyysisiä sanomia siirretään uuden pituuden mukaan ja niitä voi olla enemmän kuin ennen muutosta.

Pankit noudattavat samoja sääntöjä asiakkailta tulevien turvasanomien käsittelyssä.

4.5.2 Esimerkkejä turvasanomien jakamisesta

Oheisena esimerkkinä on SUO-sanoma, joka ensin (versio 0.71) on 177 merkkiä pitkä, ja muutoksen

yhteydessä pitenee 330:een merkkiin (versio 0.82). Esimerkissä sovelletaan turvasanomien jakosääntöjä kahdessa ympäristössä:

- toisessa (tapaus A) fyysisen sanoman maksimipituus on 80, mutta lyhyempiäkin voi käyttää,
- toisessa (tapaus B) fyysisellä sanomalla on kiinteä pituus, 300 merkkiä.

Kummassakin tapauksessa ohjelmat on tehty versioon 0.71 aikaan, ja samat ohjelmat pystyvät muuttamattomina käsittelemään version 0.82 sanomia.

Kuvissa pisteet kuvaavat loogisen sanoman sisältöä ennen muutosta ja pilkut muuttuneen sanoman uusia kenttiä. Tyhjämerkit kuvaavat fyysisen sanoman loppuosan täyttämistä tyhjämerkeillä.

Looginen sanoma ennen muutosta

177

```
>>SUO177071.....
```

Looginen sanoma muutoksen jälkeen

177

330

```
>>SUO330082.....////////////////////
```

Tapaus A ennen muutosta

80

```
>>SUO177071.....
```

80

```
.....
```

17

```
.....
```

Tapaus A muutoksen jälkeen

80

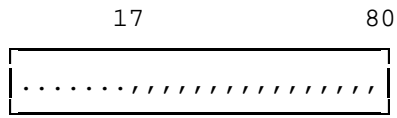
```
>>SUO330082.....
```

80

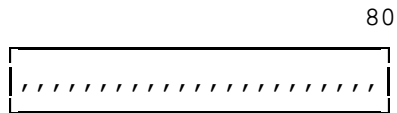
```
.....
```

Käsitellään kuten ennen

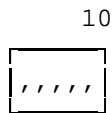
Käsitellään kuten ennen



Käsitellään kuten ennen, loppupäätä ei huomioida

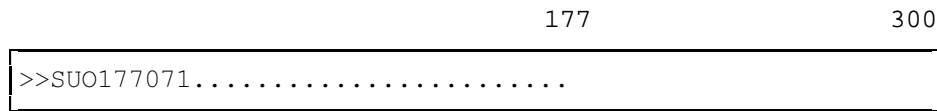


Luetaan, ei käsitellä

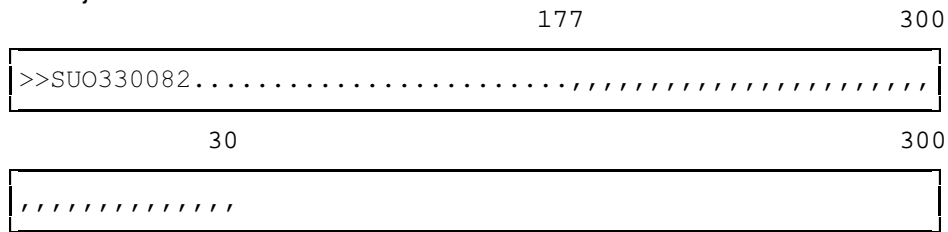


Luetaan, ei käsitellä

Tapaus B ennen muutosta



Tapaus B muutoksen jälkeen:



Ensimmäinen fyysinen sanoma käsitellään normaalisti (loppupään tietoja ei huomioida), toinen sanoma otetaan vastaan, mutta ei käsitellä.



5 TIIVISTEEN JA TARKISTEEN MUODOSTAMINEN

5.1 Tiivisteiden muodostaminen

Tiivisteiden laskennassa on kaksi menetelmää, jotka eroavat toisistaan tietueiden lopussa olevien tyhjämerkkien käsittelyn suhteen. Toista menetelmää (MENETELMÄ-koodin arvo on SKH) käytetään perinteisten aineistojen yhteydessä, toista (SKE) käytetään EDIFACT-muotoisten aineistojen yhteydessä.

Tiiviste lasketaan kaikille aineistotyypeille, joiden suojaamisesta on sovittu pankin ja asiakkaan välillä. Tiiviste muodostetaan kohtien 5.1.1- 5.1.4 kuvamalla tavalla.

5.1.1 Kerta-avaimen muodostaminen

Jokaista laskettavaa tiivistettä varten muodostetaan uusi kerta-avain, kts kohta 5.3.

Kerta-avain salakirjoitetaan yksinkertaisella DES-salakirjoituksella käyttäen siirtoavainta. Se esitetään 16:na heksamerkinä ja sijoitetaan SUO-, VAR- ja PTE-sanomaan.

5.1.2 Käsiteltävä aineistoerä

Käsiteltävä aineistoerä on pankin palvelukuvauksen mukainen aineistoerä, joka alkaa erätietueen tai muun aineistoerän alussa olevan tietueen alusta ja loppuu summatietueen tai muun aineistoerän lopussa olevan tietueen loppuun.

Tietueiden lopussa olevien tyhjämerkkien käsittelyssä on kaksi tapaa.

- SKE-menetelmässä nämä tyhjämerkit otetaan käsittelyyn mukaan.
- SKH-menetelmässä tyhjämerkit jätetään pois. Tietueen loppupäästä vasemmalle ohitetaan kaikki tyhjämerkit ensimmäiseen tyhjämerkistä poikkeavaan merkkiin asti. Ko. merkki otetaan mukaan MAC-laskentaan ja sen jälkeen siirrytään välittömästi seuraavan tietueen käsittelyyn.

5.1.3 Tietueraja ja aineistoerän loppu

Tietueiden välissä olevia rivinvaihtotms ohjausmerkkejä ei oteta mukaan MAC-laskentaan.

Tietueet käsitellään ikään kuin yhtenäisenä merkkijonona. Laskentaa varten aineistoerä jaetaan 8:n tavun lohkoihin. Jos tietueen viimeisen täyden lohkon jälkeen jää tavuja yli, ne käytetään aloittamaan seuraavan tietueen ensimmäistä lohkoa.

Jos aineistoerän viimeinen lohko jää vajaaksi, se täytetään oikealle binäärinollilla.

5.1.4 Tiiviste

Tiiviste lasketaan aineistoerästä MAC menetelmällä, kts kohta 5.5, käyttäen kerta-avainta. Käsiteltävät merkit muutetaan sisäiseen koodiin ennen MAC-laskentaa, kts 5.4.

MAC-laskennan viimeinen tuloslohko on TIIVISTE eli MAC. Se käytetään kokonaisuudessaan, 64 bittisenä, ja se esitetään 16:na heksamerkinä. Tiiviste sijoitetaan VAR- ja PTE-sanomaan.

5.2 Tarkisteen muodostaminen

ESI-, VAR- ja PTE-sanomille lasketaan tarkiste. Käsiteltävä tieto käsittää kaikki merkit sanoman alusta tarkistetta edeltävään merkkiin saakka mukaan lukien mahdolliset tyhjämerkit. Tarkisteen muodostamisessa suoritetaan seuraavat vaiheet.

Tarkiste lasketaan MAC-menetelmällä (kts. kohta 5.5) käyttäen käyttöavainta. Käsiteltävät merkit muutetaan sisäiseen koodiin ennen MAC-laskentaa, kts 5.4. Jos turvasanoma on ASCII-koodattu, niin kääntö sisäiseen koodiin ei ole tarpeen, koska käsiteltävät merkit ovat valmiina sisäisessä koodissa.

MAC-laskennan viimeinen tuloslohko on TARKISTE eli MAC. Se käytetään kokonaisuudessaan, 64 bittisenä, ja se esitetään 16:na heksamerkinä.

5.3 Kerta-avaimen muodostaminen

Tässä kuvattu menetelmä noudattaa standardin ISO8730 liitettä G. Muita menetelmiä voidaan käyttää, kunhan menetelmä on kryptograafisesti vähintään yhtä vahva.

Generoidaan satunnainen arvo (R) aikaleiman (DT) ja siemenen (V) perusteella:

$$I = e(K)(DT) \\ R = e(K)(I+V).$$



Arvon generoinnin jälkeen muodostetaan siemenelle uusi arvo:

$$V = e(K)(V+R)$$

Satunnaisen arvon (R) tavujen pariteetti asetetaan parittomaksi (kts. 6.1.3) ja lopputulos R on haluttu avain. Siemen V on talletettava ja välitettävä generoinnista toiseen.

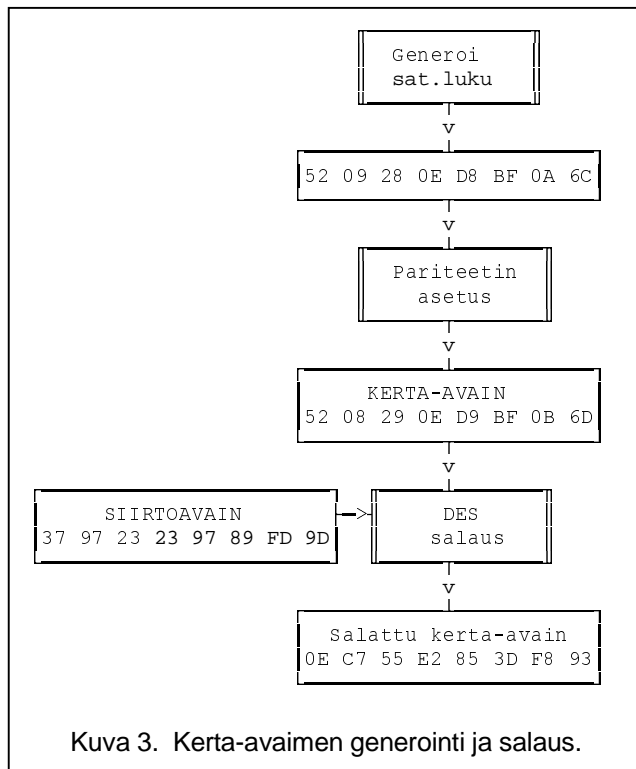
Kaavojen muuttujat ovat 64:n bitin lohkoja:

- DT, aikaleima, joka sisältää päiväyksen ja kellonajan mahdollisimman tarkkana. Uusi arvo haetaan jokaisen generoinnin yhteydessä
- I, välitulos
- R, satunnainen lohko
- V, siemen
- K, DES-avain, jota käytetään vain satunnaisavainten generointiin.

Merkinnät:

- $e(K)(x)$, x salakirjoitetaan DES:illä käyttäen avainta K.
- +, plus-merkki tarkoittaa tässä Exclusive OR operaatiota.

Avain K ja siemenen V alkuarvo muodostetaan satunnaislukuina ohjelmantekijän haluamalla tavalla. On pyrittävä antamaan niille eri arvoja eri ohjelmakopioihin ohjelmajakelumenetelmän antamien mahdollisuuksien puitteissa.



Kuva 3. Kerta-avaimen generointi ja salaus.

5.4 Sisäinen koodi

Sisäisen koodin käytöllä saadaan tiivisteiden ja tarkistusten arvon aineiston esitystavasta (ASCII tai EBCDIC) riippumattomaksi. Sisäisen koodin arvot ovat samat kuin seitsemän bittisessä ASCII-koodissa.

Pienet aakkoset ja suuret aakkoset korvataan samoilla arvoilla. Skandinaaviset merkit Å, Ä ja Ö sekä eräät erikoismerkit (esim. \$ ja #) korvataan sisäisessä koodissa samalla arvolla kuin tyhjämerkki. Sama arvo 20 annetaan kaikille merkeille, joita ei ole mainittu taulukossa.

Muunnos sisäiseen koodiin tehdään oheisen taulukon 1 mukaan. Taulukossa merkkien arvot on esitetty heksadesimaalisina.

| Nimitys | Merkki | Arvo |
|-------------------|---------|------|
| AAKKOSET | A, a | 41 |
| | B, b | 42 |
| | C, c | 43 |
| | ... | ... |
| | Y, y | 59 |
| | Z, z | 5A |
| | NUMEROT | 0 |
| | 1 | 31 |
| | 2 | 32 |
| | ... | ... |
| | 8 | 38 |
| | 9 | 39 |
| tyhjämerkki | | 20 |
| prosenttimerkki | % | 25 |
| vasen kaarisulku | (| 28 |
| oikea kaarisulku |) | 29 |
| tähti | * | 2A |
| plusmerkki | + | 2B |
| pilkku | , | 2C |
| miinusmerkki | - | 2D |
| piste | . | 2E |
| kauttaviiva | / | 2F |
| kaksoispiste | : | 3A |
| puolipiste | ; | 3B |
| pienempi kuin | < | 3C |
| yhtäläisyysmerkki | = | 3D |
| suurempi kuin | > | 3E |
| KAIKKI MUUT | | 20 |

Taulukko 1. Sisäinen koodi

5.5 MAC-laskenta

MAC lasketaan standardin ISO 8731-1 mukaisesti käyttäen DES-algoritmia, kts. kuva 4. Alustusvektoria (IV, initialization vector) ei käytetä. Jos turvalaite tai ohjelma sellaisen tarvitsee, vektori asetetaan binääri-



nolliksi. Tiivistettä laskettaessa käytetään kertaavainta, tarkistetta laskettaessa käyttöavainta.

Merkit kootaan kahdeksan (8) merkin lohkoiksi. Lohko voi alkaa yhdellä sanomalla ja jatkua seuraavalla. Ennen MAC-laskentaa tehdään muunnos sisäiseen muotoon. Jos viimeinen lohko jää vajaaksi, sen loppuosa täytetään binäärinollilla.

Laskenta noudattaa oheista kaaviota 4, jossa DATAn -lohkot ovat sisäisessä koodissa olevia käsiteltävän tiedon kahdeksan tavua pitkiä lohkoja. Ensimmäinen lohko salakirjoitetaan ja saadaan välitulos T1:

$$T1 = \text{DES}(\text{DATA1})$$

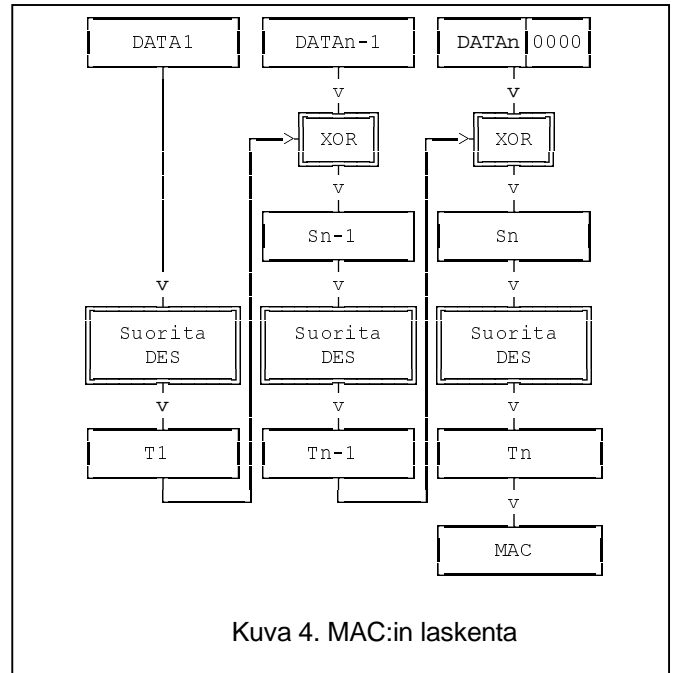
Välitulos T1 lisätään exclusive OR operaatiolla seuraavaan lohkoon:

$$S2 = T1 + \text{DATA2}$$

ja summa salakirjoitetaan:

$$T2 = \text{DES}(S2)$$

Tämä lisätään seuraavaan datalohkoon jne.



Kuva 4. MAC:in laskenta



6 AVAINHALLINTO

6.1 Yleistä

Turvaratkaisu perustuu salaisiin DES-avaimiin. PATU-menettelmässä käytetään kolmea eri avainta. Tiedostosiirron kummallakin osapuolella on omat kopionsa avaimista. Asiakkaalla on eri avaimet kutakin käyttämäänsä pankkia kohti.

6.1.1 Avaintyytit

PATUssa käytettävät avaimet ovat SIIRTO-, KÄYTTÖ- JA KERTA-AVAIN. Asiakas käsittelee vain siirtoavainta. Kaksi muuta avainta hoidetaan ohjelmiston avulla ja ne esiintyvät vain sähköisessä muodossa.

- Kerta-avainta käytetään aineistoerän tiivisteiden laskentaan. Avain luodaan jokaista suojattavaa aineistoerää varten erikseen. Avain on lukuarvoltaan satunnainen ja ainutkertainen.
- Käyttöavain on pankin antama ja sitä käytetään turvasanomien tarkisteiden laskennassa.
- Siirtoavain on pankin antama ja sitä käytetään kerta-avaimien ja käyttöavaimen salakirjoitukseen.

Kerta-avaimen generointi on kuvattu kohdassa 5.3 ja sen käyttö kohdassa 5.1. Avainten käytöstä turvasanomissa on yhteenveto kohdassa 4.2.

Asiakkaalla ja pankilla on kummallakin kopio käyttöavaimesta ja siirtoavaimesta. Ne pitävät avaimet salassa muilta osapuolilta säilyttämällä ne turvallisesti joko turvalaitteessa tai salakirjoitetuina.

Siirto- ja käyttöavaimia vaihdetaan määräväleillä (kts. 6.3 - 6.5). Siirtoavain toimitetaan asiakkaalle pape-ritulosteena postitse tai pankkikonttorin kautta. Käyttöavain toimitetaan asiakkaalle turvasanomissa sähköisessä muodossa.

6.1.2 Avaimen sukupolvinumero

Uuden käyttö- tai siirtoavaimen toimituksen jälkeen, nk. vaihtojakson aikana, avaimesta on voimassa sekä uusi että vanha versio. Saman avaimen (siirto- ja käyttöavaimet) eri versioita kutsutaan sukupolviksi ja ne erotetaan toisistaan sukupolvinumeron avulla.

Ensimmäiset avaimet, jotka asiakas ottaa käyttöön siirtyessään käyttämään PATUa, saavat sukupolvinumeron 0 (nollasukupolven avaimet). Avaimen vaihdon yhteydessä sukupolvinumeroa kasvatetaan yhdellä. Arvon 9 jälkeen käytetään arvoa 1.

Kun pankki muodostaa vastauksensa (ESI-sanoman tai PTE-sanoman) asiakkaan lähettämään turvasanomaan (ESI-sanomaan tai VAR-sanomaan), se käyttää samaa siirtoavaimen ja käyttöavaimen sukupolvea kuin asiakkaan turvasanomassa oli käytetty.

6.1.3 Avainten pariteetti

Avaimet muodostuvat kahdeksasta binääritavusta, joiden vähiten merkitsevä bitti on pariteetti-bitti. PATU:n avaimen kaikkien tavujen pariteetti asetetaan parittomaksi avaimen muodostamisen yhteydessä.

Pariteetti muodostetaan laskemalla pariteettibittiä lukuun ottamatta kunkin tavun ykkösbittien lukumäärä. Jos ykkösbittien lukumäärä on parillinen (0, 2, 4 tai 6), asetetaan tavun vähiten merkitsevä bitti ykköseksi. Jos lukumäärä on pariton (1, 3, 5 tai 7), asetetaan vähiten merkitsevä bitti nollassi.

Asiakas muodostaa pankkiin lähetettävien aineistoerien tiivisteiden laskennassa käytettävät kerta-avaimet ja pankki muodostaa kaikki muut avaimet. Vastanottaja tarkastaa avaimet ja hylkää turvasanomman, jos siinä välitettävän avaimen pariteetti on virheellinen.

Asiakas ja pankki muodostavat käyttöavaimen ns. nollasukupolven siirtoavaimen avulla (kts. 6.4). Muodostamisen yhteydessä myös nolla-avaimen pariteetti asetetaan parittomaksi.

Siirtoavaimen osilla on myös pariton pariteetti, jonka asiakkaan järjestelmä tarkastaa, kun avaimen osia syötetään järjestelmään. Varsinainen siirtoavain muodostetaan laskemalla osat yhteen Exclusive OR-operaatiolla. Summan pariteetti korjataan parittomaksi.

6.1.4 Avaintarkiste

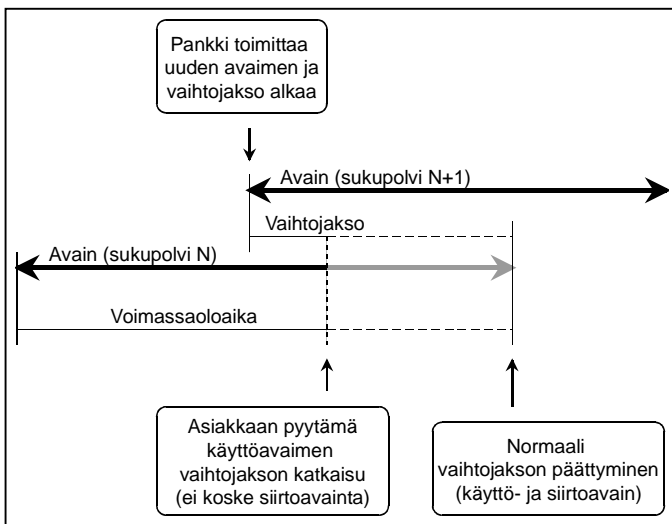
Siirtoavaimelle ja käyttöavaimelle lasketaan avaintarkiste. Tarkiste lasketaan salakirjoittamalla DES-algoritmillä kahdeksan tavua, joiden sisällöt ovat binäärinollia. Salakirjoitusavaimena käytetään avainta, jolle tarkistetta lasketaan. Salakirjoituksen tuloksen kolme ensimmäistä tavua käytetään avaintarkistena. Se esitetään kuutena heksamerkinä. Avaintarkisteen muodostus sisältyy kuvaan 8, jossa se



suoritetaan osana siirtoavaimen syöttöä. Siirtoavaimen avaintarkistetta käytetään varmistamaan, että siirtoavain on syötetty oikein asiakkaan järjestelmään.

Avaintarkisteita käytetään myös, kun asiakkaan ja pankin yhteyshenkilöt joutuvat puhumaan asiakkaan siirtoavaimista tai käyttöavaimista, esimerkiksi, jos on tarve verrata, onko kummallakin osapuolella sama avain käytössään.

6.2 Avainten jakelu ja vaihto



Kuva 5. Avainten voimassaoloaika ja vaihtojakso

Siirtoavain vaihdetaan pankin määräämällä ajoituksella. Asiakas voi halutessaan pyytää uutta siirtoavainta pankin tukikeskuksesta. Siirtoavain toimitetaan asiakkaalle kahtena osana paperitulosteena. Käyttöavain vaihdetaan turvasanomilla. Pankki lähettää uuden käyttöavaimen määräämällään ajoituksella. Asiakas voi myös pyytää avaimen vaihtoa turvasanomalla (kts. 6.2.3)

Avaimen vaihtojakso alkaa, kun pankki muodostaa uuden avaimen. Asiakas ottaa uuden avaimen käyttöönsä, kun on todennut sen virheettömästi vastaanotetuksi. Pankki ottaa uuden avaimen käyttöön, kun se havaitsee, että asiakas on sitä käyttänyt tai vaihtojakso päättyy. Vaihtojakson aikana sekä pankki että asiakas varautuvat siihen, että voidaan käyttää sekä edellistä että uutta avainta, kts. kuva 5.

6.2.1 Siirtoavaimen jakelu

Avaimet toimitetaan pankkikohtaisella menettelyllä joko postitse tai pankin konttorin kautta. Avain toimi-

tetaan kahtena eri lähetyksenä ja kahtena eri päivänä ja/tai asiakasyrityksen kahdelle eri henkilölle, jotka syöttävät avainten osat tiedostoon taltiointia varten kukin erikseen.

Avaimen osat ja avaintarkiste tulostetaan kirjekuoriin siten, että

- osan 1 kuoressa ovat tunnistetiedot sekä avaimen ensimmäinen osa
- osan 2 kuoressa ovat tunnistetiedot, avaimen toinen osa sekä avaintarkiste

Pankkien avaintulosteet noudattavat soveltuvin osin oheista kuvien 6 ja 7 mukaista mallia.

Siirtoavaimen osa 1 tulostetaan kuvan 6 osoitamalla tavalla.

| | |
|--|-------------------------|
| Asiakkaan nimi pp.kk.vvvv Kohdistintieto | |
| Pankin nimi/tarkenne | |
| PANKKITUNNUS: | xxxxxxxxxxxxxxxxxxxx |
| AVAINSUKUPOLVI: | x |
| SIIRTOAVAIN,OSA1: | xx xx xx xx xx xx xx xx |

Kuva 6. Avaimen osa 1

Siirtoavaimen osa 2 tulostetaan kuvan 7 osoittamalla tavalla:

| | |
|--|-------------------------|
| Asiakkaan nimi pp.kk.vvvv Kohdistintieto | |
| Pankin nimi/tarkenne | |
| PANKKITUNNUS: | xxxxxxxxxxxxxxxxxxxx |
| AVAINSUKUPOLVI: | x |
| SIIRTOAVAIN,OSA2: | xx xx xx xx xx xx xx xx |
| AVAINTARKISTE: | xxxxxx |

Kuva 7. Avaimen osa 2.

Reunustettu osa näkyy kirjekuoren päällä, muut tiedot eivät näy ulos. Suurilla kirjaimilla olevat teks-



tit ovat vakiotekstejä. Otsikossa oleva päivämäärä on avaimen muodostamispäivämäärä, joka samalla on vaihtojakson alkupäivä. Päivämäärä on sama kummassakin avainosassa, vaikka ne lähetään asiakkaalle eri päivinä.

Asiakkaan tunnus, TUNNUS ja TARKENNE -kentät, eivät esiinny kokonaisuudessaan avaintulosteessa. Kohdistintietona käytetään osaa asiakastunnuksesta. SIIRTOAVAIN, OSAx on syötettäväksi tarkoitettu DES-avain. Avain esitetään kahden heksamerkin ryhminä, jotka erotetaan tyhjämerkillä.

6.2.2 Siirtoavaimen syöttö

Uuden siirtoavaimen tietojen syötön yhteydessä tehtävät toimenpiteet riippuvat avaimen syöttöön johdaneista syistä. Syöttö voi liittyä:

- normaaliin määräaikaiseen avaimen vaihtoon
- PATUn ensimmäiseen käyttöönottoon tai siihen rinnastettavaan käyttöavaimen kadottamisesta johtuvaan PATUn uudelleen käynnistykseen.

Siirtoavaimen syöttäminen asiakkaan järjestelmään on esitetty kuvassa 8. Pariteettitarkastuksessa tai avaintarkisteen vertailussa havaittu virhe korjataan tarkistamalla syötettyjä tietoja. Jos virhettä ei saada korjattua, on otettava yhteys pankkiin.

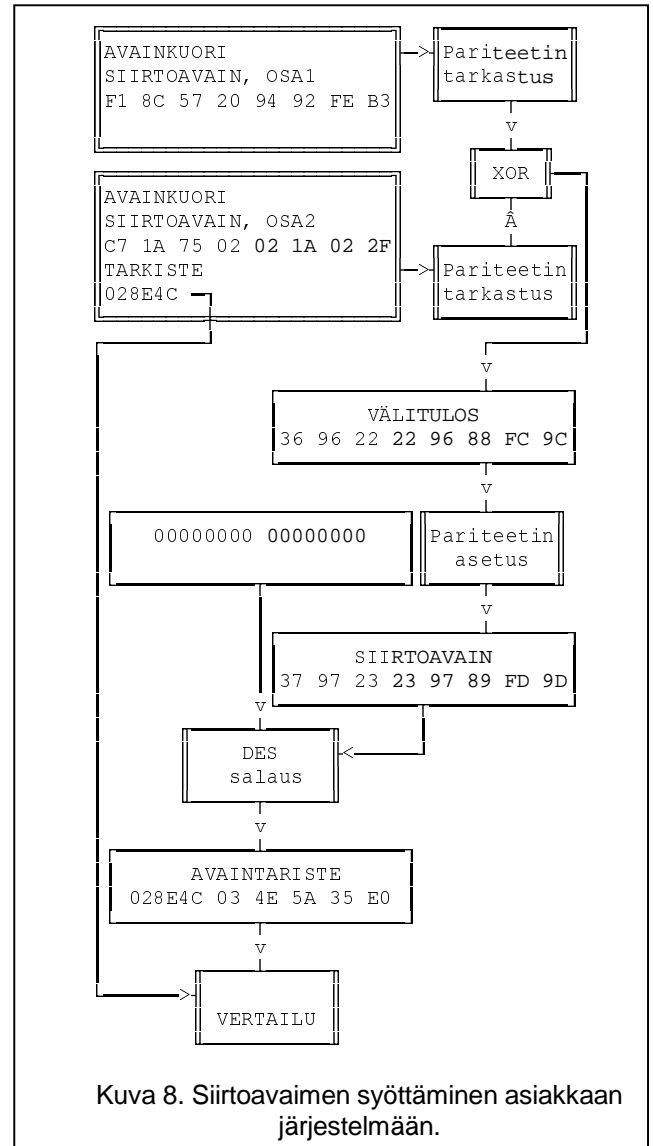
Siirtoavaimen osat on voitava syöttää eri aikaan asiakkaan järjestelmään. Siirtoavaimen osan syöttövaiheessa tarkastetaan, että tavuilla on pariton pariteetti. Toisen osan yhteydessä syötetään myös avaintarkiste. Avainsukupolvi on myös syötettävä.

Kun molemmat osat on syötetty, siirtoavain muodostetaan laskemalla osat yhteen Exclusive OR -operaatiolla. Yhdistetyn avaimen tavujen pariteetit asetetaan parittomiksi. Asiakkaan järjestelmä laskee avaintarkisteen, jonka pitää täsmätä syötetyn tarkisteen kanssa.

I. Normaali siirtoavaimen vaihto

Avaimen sukupolvinumero tarkastetaan siirtoavaimen syöttämisen yhteydessä.

- Jos avaimen sukupolvinumero on varhaisempi kuin käytössä oleva, avaimen syöttö keskeytetään ja siitä annetaan virheilmoitus
- Jos siirtoavaimen sukupolvinumero on sama kuin käytössä olevan avaimen sukupolvinumero, siitä annetaan ilmoitus. Asiakas voi kuitenkin tarvittaessa hyväksyä käytössä olevan avaimen uudelleen syötön. Avaimen uudelleen syöttö ei



Kuva 8. Siirtoavaimen syöttäminen asiakkaan järjestelmään.

vaikuta avaimen vaihtojakson pituuteen eikä muuta avaimen sukupolvinumeroa.

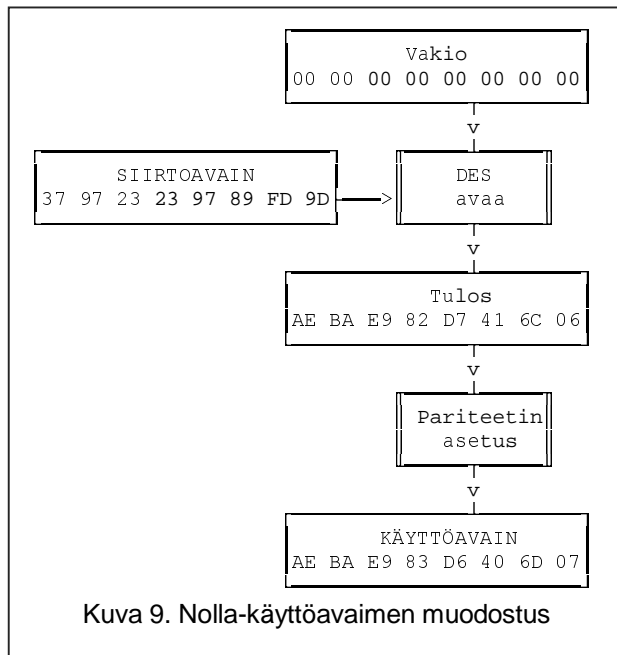
- Uuden avaimen avainsukupolven pitää olla käytössä olevasta siirtoavaimesta seuraava. (kts 6.1.2). Avaimen hyväksymisestä annetaan ilmoitus.

II. Ensimmäisen siirtoavaimen syöttö tai toiminnan uudelleenkäynnistys

Ensimmäisen siirtoavaimen syötössä ja PATU-toiminnan uudelleenkäynnistykseen yhteydessä noudatetaan samaa menettelyä. PATUn uudelleen käynnistys edellyttää, että asiakas sopii asiasta ennakkoon pankin kanssa.



- 1) Pankin viimeksi toimittama siirtoavain ja sen sukupolvinumero syötetään järjestelmään edellä kuvatulla tavalla.
- 2) Ensimmäinen käyttöavain, ns. nolla-avain, muodostetaan suoraan tästä siirtoavaimesta. Käyttöavain saadaan avaamalla siirtoavaimella tieto, jonka arvo on binäärinollia. Tulokselle asetetaan pariton pariteetti ja avaimen sukupolvinumeroksi nolla, kts. kuva 9.



6.2.3 Käyttöavaimen vaihto

Käyttöavaimen vaihto voi alkaa joko pankin aloitteesta tai asiakkaan pyytämänä. Käyttöavain jaellaan ESI-, VAR- tai PTE-sanomassa siirtoavaimella salakirjoitettuna.

Pankki voi antaa uuden, mutta sisällöltään identtisen, avaimen useamman kerran. Pankki toimittaa avaimen vastauksissaan sellaisiin turvasanomiin, joissa asiakas käyttää vanhaa käyttöavainta.

Käyttöavaimen edellinen sukupolvi on voimassa pankkikohtaisesti määritellyn voimassaoloajan loppuun, ellei asiakas erikseen pyydä vaihtojakson katkaisua (kts. kuva 5).

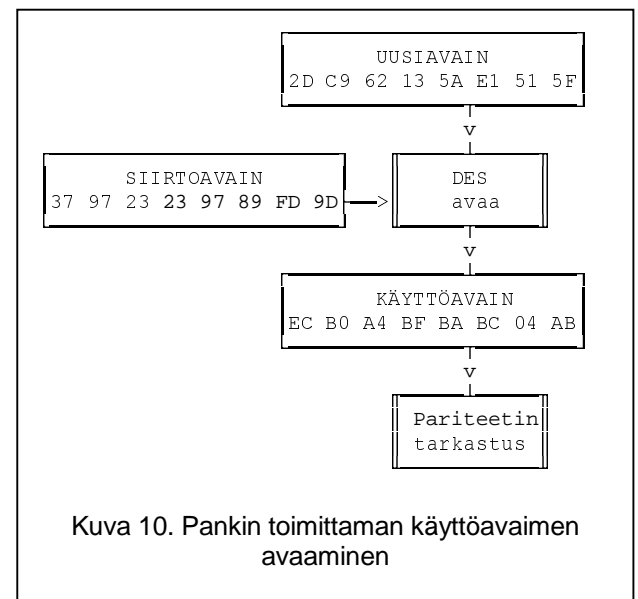
Käsittelyä ohjataan turvasanomien AVAINVAIHTO-koodilla. Pankki lähettää asiakkaalle uuden käyttöavaimen asettamalla AVAINVAIHTO-koodin arvoksi 1 ja uuden käyttöavaimen avaimen siirtoavaimella salakirjoitettuna kenttään UUSIAVAIN. Käytetyn

siirtoavaimen sukupolvinumero on kentässä SIIRTOAVAINNO.

Asiakas avaa UUSIAVAIN kentän sisällön vastaavalla siirtoavaimella, kts. kuva 10. Tulos on uusi käyttöavain, ja se saa sukupolvinumeron, joka on KÄYTTÖAVAINNO-kentässä oleva arvo lisätynä yhdellä tai numeron 1, jos vanha arvo oli 9.

Asiakas tarkastaa pankin toimittaman avaimen pariteetin. Jos uuden avaimen pariteetti on pariton, asiakas tallettaa avaimen ja alkaa käyttää sitä.

Pankki alkaa käyttää uutta avainta, kun se on vastaanottanut uudella avaimella suojatun esittäytymisen tai aineistoerän asiakkaalta. Pankin ja asiakkaan tulee edelleen kyetä vastaanottamaan vanhalla avaimella suojattuja turvasanomiam vaihtojakson loppuun asti.



6.2.4 Asiakkaan pyytämä käyttöavaimen vaihto

Asiakas voi pyytää uutta käyttöavainta asettamalla AVAINVAIHTO-koodin ykköseksi ESI- tai VAR-sanomassa.

Pankki lähettää uuden avaimen vastauksessaan:

- a) Omassa ESI-sanomassaan, jos asiakas pyytää avainvaihtoa ESI-sanomalla.
- b) Ko. aineistoerään liittyvässä PTE-sanomassa, jos asiakas pyytää avainvaihtoa VAR-sanomalla.

Ellei pankki voi toteuttaa pyydettyä avainvaihtoa, se vastaa turvasanomalla, jossa AVAINVAIHTO-koodi



on nolla. Sanomassa on silloin myös vastaava virheilmoitus. Asiakkaan lähettämää koko sanomaa tai aineistoerää ei tällöin kuitenkaan hylätä, jos se muuten on kunnossa.

6.2.5 Vaihtojakson katkaiseminen

Asiakas voi katkaista meneillään olevan vaihtojakson asettamalla turvasanomissa olevan AVAINVAIHTOKENTTÄÄN arvon 2. Tällöin kyseisessä sanomassa käytössä olevaa käyttöavainta edeltäneen käyttöavaimen voimassaolo päättyy pankin otettua pyynnön sisältäneen turvasanomien hyväksytysti vastaan.

6.3 Turvamenetelmien käyttöönottoon liittyvät toimenpiteet

Testauksessa asiakas voi käyttää testiasiakastunnuksia pankkikohtaisten ohjeiden mukaisesti. Pankit julkistavat testiasiakkaiden siirto- ja käyttöavaimet ohjeissaan..

Vanha asiakas voi käyttää rinnakkain vanhaa ja uutta tiedostosiirron menetelmää pankin kanssa sovitun päivään asti.



7 ILMOITUSKODIT

Pankkien järjestelmät antavat virhe- ja muita ilmoituksia lähettämissään ESI- ja PTE-sanomissa. ESI-sanoman ilmoitukset koskevat asiakkaan lähettämää ESI-sanomaa. PTE-sanoman ilmoitukset koskevat asiakkaan lähettämiä SUO- ja VAR-sanomia.

Tietokentät ILMOITUSKODI ja ILMOITUS välittävät virhe- ja muita ilmoituksia. ILMOITUS sisältää ilmoituskoodia vastaavan ihmiselle luettavaksi tarkoitettun selväkielisen tekstin ja sen sisältö on muotoa:

- kellonaika muodossa HH:MM:SS,
- yksi tyhjämerkki ja
- ilmoitusteksti.

Jos ONNISTUMISKODI on E, kyseessä on virhetilanne, jolloin asiakkaan esittäytyminen tai aineistoerä on hylätty.

Ilmoituskoodit jaetaan neljään ryhmään ("merkintä A <= B" tarkoittaa "B on suurempi tai yhtä suuri kuin A"):

- 1) pankin omat: ilmoituskoodi < 1000
- 2) pankin käyttämät PATU-määrittelyn mukaiset: 1000 <= ilmoituskoodi < 2000

- 3) pankkiyhteysohjelman tai asiakkaan omat: 2000 <= ilmoituskoodi < 3000

- 4) pankkiyhteysohjelman tai asiakkaan PATU-määrittelyn mukaiset: 3000 <= ilmoituskoodi < 4000.

PATU-määrittelyn ilmoituskoodi- ja tekstitaulukossa taulukko 2) käytetään seuraavia lyhenteitä:

- R korvataan ryhmänumerolla
- NNN kentän nimi
- VVV kentän arvo.

Näitä PATU-määrittelyn ilmoituskoodeja ja -tekstejä tulisi käyttää sekä pankin järjestelmissä että asiakkaan pankkiyhteysohjelmissa. Pankkiyhteysohjelman tulisi välittää pankin antamat ilmoituskoodit ja -tekstit sellaisenaan eteenpäin (esim. lokiin tai näyttöön).

Esimerkiksi, jos pankki havaitsee, että asiakkaan ESI-sanomassa aikaleiman päiväys on liian vanha, pankki ilmoittaa tästä asiakkaalle vastaavassa pankin ESI-sanomassa ilmoituskoodilla 1015.

Esimerkiksi, jos pankkiyhteysohjelma havaitsee, että PTE-sanomassa TARKISTE ei täsmää, tämä ilmoitetaan koodilla 3020 joko käyttäjälle tai kirjoittamalla tieto virhelokiin.



| Ilmoitus- koodi | Ilmoitusteksti | Onnistumis- koodi |
|--------------------|---|----------------------|
| R001 | HYVÄKSYTTY | K |
| R002 | HYVÄKSYTTY, AVAINVAIHTO | K |
| R003 | HYVÄKSYTTY, AVAINVAIHTO HYVÄKSYTTY | K |
| R004 | HYVÄKSYTTY, AVAINVAIHTO HYLÄTTY | K |
| R005 | HYVÄKSYTTY, AVAINVAIHTO LIIAN USEIN | K |
| R010 | MUOTOVIRHE KENTÄSSÄ NNN VVV | E |
| R011 | ARVOVIRHE KENTÄSSÄ NNN VVV | E |
| R012 | VERSIO ON LIIAN VANHA | E |
| R013 | SIIRTOAVAIN EI OLE VOIMASSA | E |
| R014 | KÄYTTÖAVAIN EI OLE VOIMASSA | E |
| R015 | PÄIVÄYS ON LIIAN VANHA | E |
| R016 | PÄIVÄYS ON ETEENPÄIN | E |
| R017 | KERTA-AVAIN ON JO KÄYTETTY | E |
| R018 | AIKALEIMA ON JO KÄYTETTY | E |
| R019 | TIIVISTE EI TÄSMÄÄ | E |
| R020 | TARKISTE EI TÄSMÄÄ | E |
| R021 | VASTAANOTTAJA ON VÄÄRIN | E |
| R022 | ESI-AIKALEIMAT EIVÄT TÄSMÄÄ | E |
| R023 | SUO-SANOMA PUUTTUU | E |
| R024 | VAR-SANOMA PUUTTUU | E |
| R025 | SUOJAUSOIKEUTTA EI OLE | E |
| R026 | KENTTÄ NNN: SUO-SANOMA <> VAR-SANOMA | E |
| R027 | KENTTÄ NNN: SUO-SANOMA <> PTE-SANOMA | E |
| R028 | KENTTÄ TIIVISTE: VAR-SANOMA <> PTE-SANOMA | E |
| R029 | PTE-SANOMA PUUTTUU | E |
| R030 | KÄYTTÖAVAIMEN PARITEETTI EI TÄSMÄÄ | E |
| R031 | KERTA-AVAIMEN PARITEETTI EI TÄSMÄÄ | E |
| R032 | TURVASANOMA LIIAN LYHYT | E |
| R033 | ASIAKASTUNNUS VIRHEELLINEN | E |
| R034 | JÄRJESTELMÄVIRHE | E |
| R035 | PATUN KÄYTÖSTÄ EI OLE SOVITTU | E |
| R036 | HYVÄKSYTTY, VAIHTOJAKSO KATKAISTU | K |
| R037 | HYVÄKSYTTY, VAIHTOJAKSON KATKAISU HYLÄTTY | K |

Taulukko 2 Ilmoituskoodit ja -tekstit



LIITE 1

TURVASANOMIEN TIEDOT

Turvasanomissa käytettävät tiedot on lueteltu oheisessa taulukossa L1-1.

| Tiedon numero | Nimi | Muoto | Selitys | | | | | | | | |
|---------------------------------|---------------------------|--------|---|----------|---------|--------------------|------------------|------------------------------|---------------------------|---------------------------------|---|
| 1 | SANOMATUNNUS | AN(5) | Turvasanomien tunnus: <ul style="list-style-type: none"> >>ESI = Esittäytymissanoma >>SUO = Suojausotsake >>VAR = Suojauslopuke >>PTE = Palautesanoma | | | | | | | | |
| 2 | SANOMAPITUUS | N(3) | Sanoman pituus merkkeinä | | | | | | | | |
| 3 | VERSIO | N(3) | Turvastandardin versio, (Hyväksyttävät arvot 110 ja 120) esim. versiossa (V1.2) sanomassa 120 | | | | | | | | |
| 4 | ONNISTUMISKOODI | AN(1) | Pankin lähettämä koodi: <ul style="list-style-type: none"> K = turvasanoma ja mahdollinen aineistoerän suojaus hyväksytty E = turvasanoma tai aineistoerän suojaus hylätty | | | | | | | | |
| 5 | ILMOITUSKOODI | N(4) | Virhe- tai ilmoituskoodi, kts. kohta 7 | | | | | | | | |
| 6 | OHJELMISTO | AN(16) | Vapaamuotoinen teksti, joka kertoo lähettävän ohjelmiston ja version, ei saa olla kokonaan tyhjää. Esim.: <ul style="list-style-type: none"> Asiakkaalta: "PANKSOFT 4.1" Pankista: "PANKKILINJA 3.5" | | | | | | | | |
| 7 | MENETELMÄ | AN(3) | Turvamenetelmää yksilöivä koodi: <ul style="list-style-type: none"> SKH = tiivisteen laskennan menetelmä, jossa tietueen lopussa olevat tyhjämerkit poistetaan SKE = tiivisteen laskennan menetelmä, jossa tietueen lopussa olevia tyhjämerkkejä ei poisteta SMH = tarkisteen laskennan menetelmä | | | | | | | | |
| 8 | VASTAANOTTAJA | | Vastaanottajan tunniste: | | | | | | | | |
| 8.1 | VAST.TUNNUS | AN(17) | <ul style="list-style-type: none">Pankin antama pankin tunnus tai pankin antama asiakastunnus | | | | | | | | |
| 8.2 | VAST.TARKENNE | AN(8) | <ul style="list-style-type: none">Tyhjää tai pankin antama asiakkaan tai pankin tarkentava tieto | | | | | | | | |
| 9 | LÄHETTÄJÄ | | Lähettäjän tunniste: | | | | | | | | |
| 9.1 | LÄH.TUNNUS | AN(17) | <ul style="list-style-type: none">Pankin antama pankin tunnus tai pankin antama asiakastunnus | | | | | | | | |
| 9.2 | LÄH.TARKENNE | AN(8) | <ul style="list-style-type: none">Tyhjää tai pankin antama asiakkaan tai pankin tarkentava tieto | | | | | | | | |
| 10 | SIIRTOAVAINNO | N(1) | Siirtoavaimen sukupolvinumero, kts 6.1.2 | | | | | | | | |
| 11 | KÄYTTÖAVAINNO | N(1) | Käyttöavaimen sukupolvinumero, kts 6.1.2 | | | | | | | | |
| 12 | AIKALEIMA | | Turvasanomien aikaleima: | | | | | | | | |
| 12.1 | PÄIVÄYS | N(6) | <ul style="list-style-type: none">Päiväys muodossa vvkppp | | | | | | | | |
| 12.2 | KELLONAIKA | N(6) | <ul style="list-style-type: none">Kellonaika muodossa hhmss | | | | | | | | |
| 12.3 | LEIMANUMERO | N(3) | <ul style="list-style-type: none">Aikaleiman ainutkertaiseksi tekevä numero, nolliä, ellei tarvita | | | | | | | | |
| 13 | SUOJAUSALUE | AN | <ul style="list-style-type: none"> S = siirtoeräkohtainen suojaus A = aineistoeräkohtainen suojaus, kts. kohta 3.5.4 | | | | | | | | |
| 14 | VARALLA | AN(9) | Ei käytössä | | | | | | | | |
| 15 | KERTA-AVAIN | AN(16) | Kerta-avain salakirjoitettuna, heksadesimaalisena | | | | | | | | |
| 16 | TIIVISTE | AN(16) | Aineistoerän tiiviste (MAC) heksadesimaalisena | | | | | | | | |
| 17 | TARKISTE | AN(16) | Tämän turvasanomien tarkiste (MAC) heksamerkkeinä | | | | | | | | |
| 18 | AVAINVAIHTO | AN(1) | Käyttöavaimen vaihtopyyntö: <table border="0"> <tr> <td>Asiakas:</td> <td>Pankki:</td> </tr> <tr> <td>0 Ei toimenpiteitä</td> <td>Ei toimenpiteitä</td> </tr> <tr> <td>1 Haluan uuden käyttöavaimen</td> <td>Tässä on uusi käyttöavain</td> </tr> <tr> <td>2 Haluan katkaista vaihtojakson</td> <td>-</td> </tr> </table> | Asiakas: | Pankki: | 0 Ei toimenpiteitä | Ei toimenpiteitä | 1 Haluan uuden käyttöavaimen | Tässä on uusi käyttöavain | 2 Haluan katkaista vaihtojakson | - |
| Asiakas: | Pankki: | | | | | | | | | | |
| 0 Ei toimenpiteitä | Ei toimenpiteitä | | | | | | | | | | |
| 1 Haluan uuden käyttöavaimen | Tässä on uusi käyttöavain | | | | | | | | | | |
| 2 Haluan katkaista vaihtojakson | - | | | | | | | | | | |
| 19 | UUSIAVAIN | AN(16) | Käyttöavain salakirjoitettuna, heksadesimaalisena | | | | | | | | |



| | | | |
|----|----------|--------|--|
| 20 | ILMOITUS | AN(60) | Virhettä tai muuta tilannetta kuvaava selväkielinen teksti |
| 21 | KUITTAUS | AN(80) | Nykyjärjestelmissä käytössä oleva koontisummasanoma |

Taulukko L1-1. Turvasanomien tiedot

Kentissä 1 - 16 saa käyttää ainoastaan sisäisessä kooditaulukossa lueteltuja merkkejä lukuun ottamatta pieniä kirjaimia, kts. kohta 6 taulukko 2.



LIITE 2

TURVASANOMISSA KÄYTETTÄVÄT TIETOKENTÄT

Eri turvasanomissa käytettävät tietokentät on esitetty oheisessa taulukossa L2-1.

| Tiedon numero | Kentän nimi | Turvasanomien: | | | | | |
|---------------|-----------------|----------------|------|-----|------|------|-----|
| | | ESla | ESlp | SUO | VARa | VARp | PTE |
| 1 | SANOMATUNNUS | X | X | X | X | X | X |
| 2 | SANOMAPITUUS | X | X | X | X | X | X |
| 3 | VERSIO | X | X | X | X | X | X |
| 4 | ONNISTUMISKOODI | o | X | o | o | o | X |
| 5 | ILMOITUSKOODI | o | X | o | o | o | X |
| 6 | OHJELMISTO | X | X | X | X | X | X |
| 7 | MENETELMÄ | X | X | X | X | X | X |
| 8 | VASTAANOTTAJA | X | X | X | X | X | X |
| 9 | LÄHETTÄJÄ | X | X | X | X | X | X |
| 10 | SIIRTOAVAINNO | X | X | X | X | X | X |
| 11 | KÄYTTÖAVAINNO | X | X | X | X | X | X |
| 12 | AIKALEIMA | X | X | X | X | X | X |
| 13 | SUOJAUSALUE | o | o | X | X | X | X |
| 14 | VARALLA | o | o | o | o | o | o |
| 15 | KERTA-AVAIN | o | o | X | X | X | X |
| 16 | TIIVISTE | o | o | - | X | X | X |
| 17 | TARKISTE | X | X | - | X | X | X |
| 18 | AVAINVAIHTO | X | X | - | X | X | X |
| 19 | UUSIAVAIN | - | X | - | - | X | X |
| 20 | ILMOITUS | - | X | - | - | X | X |
| 21 | KUITTAUS | - | - | - | - | - | X |
| | Tietuepituus | 161 | 237 | 128 | 161 | 237 | 317 |

Merkintöjen selitykset:

- X = käytössä
- o = ei käytössä (tyhjämerkkejä tai nollia)
- - = ei mukana sanomassa

SUO-sanomassa MENETELMÄ-kenttä ilmaisee tiivisteen laskennan menetelmän ja muissa sanomissa tarkisteen laskentamenetelmän.



LIITE 3

ESIMERKKI TURVASANOMIEN KÄYTÖSTÄ JA SISÄLLÖSTÄ

Turvasanomien on esimerkissä jaettu 80-merkin pituisiin riveihin.

Pankin antamat tunnukset:

- asiakastunnus: 999100000111111111
- pankin tunnus: 003701234567

Siirto-avain 0:

- osa 1: F1 8C 57 20 94 92 FE B3
- osa 2: C7 1A 75 02 02 1A 02 2F
- tarkiste: 02 8E 4C

Käyttöavain 0 (laskettuna siirto-avaimesta):
AE BA E9 83 D6 40 6D 07

Asiakkaan pankkiin lähettämä esittäytymissanoma (ESla):

```

-----1-----2-----3-----4-----5-----6-----7-----8
>>ESI161120 0000KERMIT      3.01SMH003701234567      999100000111111111
      00941015073000001      4B69B6DD4F72C75B
0
-----1-----2-----3-----4-----5-----6-----7-----8

```

Asiakkaan pankista saama vastaus (ESlp):

```

-----1-----2-----3-----4-----5-----6-----7-----8
>>ESI237120K1002PANKKILINJA 1.20SMH999100000111111111      003701234567
      00941015073000001      FC13A419E2BBE1C5
12DC962135AE1515F07:32:15 HYVÄKSYTTY, AVAINVAIHTO
-----1-----2-----3-----4-----5-----6-----7-----8

```

Suojattu aineisto (kerta-avain: 52 08 29 0E D9 BF 0B 6D)

```

-----1-----2-----3-----4-----5-----6-----7-----8
>>SUO128120 0000KERMIT      3.01SKH003701234567      999100000111111111
      00941015073125001S      0EC755E2853DF893
1921030 259018000000140111111116100000000121MATTI MEIKÄLÄINEN 010101001A
1921030 259018000000140111111116100000000321MAIJA MEIK#L#INEN 010201001A
1921030 259018000000140111111116100000000421Ä. Ö. ÄLAND 010101001A
1921030 259018000000140111111116100000000521#. @. $LAND 010101001A
4921030 0111111116100000001384 000004
>>VAR161120 0000KERMIT      3.01SMH003701234567      999100000111111111
      00941015073125001S      0EC755E2853DF8934954F0194C2B696D91B78D377B4F70D1
0
-----1-----2-----3-----4-----5-----6-----7-----8

```

Asiakkaan pankista saama PTE-vastaus:

```

-----1-----2-----3-----4-----5-----6-----7-----8
>>PTE317120K1002PANKKILINJA 1.20SMH999100000111111111      003701234567
      00941015073125001S      0EC755E2853DF8934954F0194C2B696D359D012A52A6FD2E
12DC962135AE1515F07:32:15 HYVÄKSYTTY, AVAINVAIHTO      TS
      0010000040000000000001384+00000000000000000000000000000000+921015073214
-----1-----2-----3-----4-----5-----6-----7-----8

```