(19) SUOMI - FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN
FINNISH PATENT AND REGISTRATION OFFICE

(10) **FI 127624 B**
(12) **PATENTTIJULKAISU**
PATENTSKRIFT
PATENT SPECIFICATION

(45) Patentti myönnetty - Patent beviljats - Patent granted **31.10.2018**

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
G06Q 20/38 (2012.01)
G06Q 20/02 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/26 (2012.01)

(21) Patenttihakemus - Patentansökning - Patent application 20165360

(22) Tekemispäivä - Ingivningsdag - Filing date **25.04.2016**

(23) Saapumispäivä - Ankomstdag - Reception date **25.04.2016**

(43) Tullut julkiseksi - Blivit offentlig - Available to the public **26.10.2017**

(73) Haltija - Innehavare - Proprietor
1 •Gurulogic Microsystems Oy, Linnankatu 34, 20100 TURKU, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare - Inventor
1 •Kärkkäinen, Tuomas, TURKU, SUOMI - FINLAND, (FI)
2 •Kalevo, Ossi, TURKU, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud - Agent
Kolster Oy Ab, Salmisaarenaukio 1, 00180 Helsinki

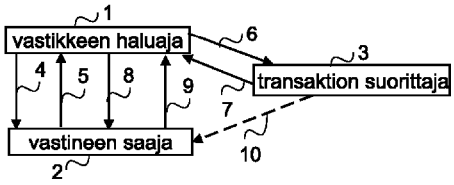
(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention
Transaktiojärjestely
Transaktionsarrangemang
Transaction arrangement

(56) Viitejulkaisut - Anförda publikationer - References cited
US 2015199684 A1, US 2011184867 A1, US 2006224508 A1, US 2007005613 A1, US 2013097081 A1

(57) Tiivistelmä - Sammandrag - Abstract

Reaaliaikainen vastikkeellinen transaktio toteutetaan siten, että kun vastikkeen haluaja saa (1) tiedon vastineesta (5) vastikkeen haltijalta eli vastineen saajalta (2), välittää vastikkeen haluaja (1) vastineen ja saajan tiedot (6) suojatulla yhteydellä transaktion suorittajalle (3), joka palauttaa tiedon transaktion onnistumisesta (7) vastikkeen haluajalle (1).

Transaktion mot betalning i realtid förverkligas så att när den som önskar en betalning får (1) information om en ersättning (5) från betalningsinnehavaren dvs. ersättningsmottagaren (2), förmedlar den (1) som önskar en betalning ersättningen och mottagarens data (6) med en skyddad förbindelse till utföraren (3) av transaktionen, vilken utförare returnerar data om en lyckad transaktion (7) till den (1) som önskar en betalning.



Transaktiojärjestely

Keksinnön ala

Keksintö liittyy reaaliaikaisen vastikkeellisen transaktion toteuttamiseen ja erityisesti siinä tarvittavien tietojen välittämiseen.

Keksinnön tausta

Tietoliikennetekniikan kehittymisen myötä iso osa erilaisista vastikkeellisista transaktioista on siirtynyt sähköisesti hoidettavaksi. Esimerkkejä sovelluksista, joita käytetään vastikkeellisiin transaktioihin, ovat mobiilimaksamiseen liittyvät sovellukset, kuten maksaminen tekstiviestin avulla, älypuhelimissa toimiva mobiilirahakukkaro tai mobiililuottokortti. Tyypillisesti tekstiviestimaksamisessa maksu välitetään myyjälle matkapuhelinoperaattorin kautta, joka puolestaan lisää laskun puhelinmaksuun. Mobiilirahakukkarossa käytetään etukäteen sähköiseen kukkaroon verkkopankista siirrettyä rahaa, ja maksu suoritetaan sähköisestä kukkarosta lähettämällä tekstiviestinä avainsana palvelunumeroon tai lähilukemalla esimerkiksi NFC (Near Field Communication) -tekniikkaa tai jotain muuta RFID (Radio Frequency Identification) -tekniikkaan perustuvaa ratkaisua hyödyntäen. Mobiililuottokorttisovellus on esimerkki pilvipohjaisesta maksamisesta ja eroaa mobiilirahakukkarosta siinä, että se lähettää sekä rahaa suoraan vastaanottajan tilille että laskun älypuhelimen mobiililuottokortin käyttäjäksi rekisteröineelle henkilölle. Tunnetuissa ratkaisuissa maksun saajan täytyy tukea käytettyä tekniikkaa ja maksajan täytyy joko etukäteen siirtää rahaa päätelaitteeseensa tai maksajan täytyy maksaa luotollisen palvelun kautta, johon maksaja on aikaisemmin rekisteröitynyt. Siirrettäessä rahaa etukäteen päätelaitteeseen tai maksettaessa luotollisen palvelun kautta ratkaisu ei ole maksajan kannalta reaaliaikainen, sillä varsinainen tiliä veloittava transaktio tapahtuu eri aikaan.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on kehittää reaaliaikainen vastikkeellisen transaktion suorittava sovellus. Keksinnön tavoite saavutetaan menetelmällä, päätelaitteella ja järjestelmällä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuviot 1A ja 1B esittävät yksinkertaistettuja yleisluontoisia järjestelmäarkkitehtuureja;

Kuvio 2 on vuokaavio, joka havainnollistaa esimerkinomaista toiminnollisuutta;

Kuviot 3A ja 3B esittävät yksinkertaistettua tiedonsiirtoa ja toiminnollisuutta eräässä esimerkissä;

Kuvio 4 esittää yksinkertaistettua tiedonsiirtoa ja toiminnallisuutta eräässä toisessa esimerkissä;

Kuviot 5A ja 5B esittävät transaktion vastineen vastaanottajan järjestelmän eri osien toiminnollisuutta vielä eräässä erilaisessa esimerkissä

Kuvio 6 esittää esimerkin vastikkeellisen reaaliaikaisen transaktion ketjusta;

Kuviot 7A-7C havainnollistavat erilaisia käyttöliittymänäkymiä; ja

Kuvio 8 on yksinkertaistettu lohkokaavio käyttäjän päätelaitteesta; ja

Kuvio 9 on yksinkertaistettu lohkokaavio siirtopalvelimesta; ja

Kuvio 10 on yksinkertaistettu lohkokaavio transaktion vastineen vastaanottajan laitteistosta.

Keksinnön yksityiskohtainen selostus

Seuraavat suoritusmuodot ovat esimerkinomaisia. Vaikka selitys voi viitata useassa paikassa "erääseen", "yhteen" tai "johonkin" suoritusmuotoon ja/tai esimerkkiin (suoritusmuotoihin/esimerkkeihin), ei tämä välttämättä tarkoita, että kukin sellainen viittaus on samaan suoritusmuotoon (suoritusmuotoihin) ja/tai esimerkkiin (esimerkkeihin) tai että piirre soveltuu vain yhteen suoritusmuotoon ja/tai esimerkkiin. Eri suoritusmuotojen ja esimerkkien yksittäisiä piirteitä voidaan myös yhdistää aikaansaamaan muita suoritusmuotoja ja esimerkkejä. Tulee myös ymmärtää, että jotkut toiminnot, rakenteet ja elementit, joita käytetään kontekstin luomiseksi selostettaville suoritusmuodoille ja/tai esimerkeille voivat sellaisinaan olla epärelevantteja itse keksinnölle. Seuraavan selostuksen rakenteiden, sanojen ja ilmausten onkin tarkoitus havainnollistaa eikä rajoittaa keksintöä tai sen suoritusmuotoja.

Keksintöä selostetaan seuraavassa käyttäen esimerkkinä reaaliaikaisesta vastikkeellisesta transaktiojärjestelystä suoramaksusovellusta rajoittamatta esimerkkejä siihen.

Kuvioissa 1A ja 1B havainnollistetaan erään suoritusmuodon mukaista yleistä arkkitehtuuria, joka esittää vain joitakin tietoliikennejärjestelmän 100 elementtejä ja toiminnallisia yksiköitä. Kuvioissa 1A ja 1B esitetyt kytkennät ja yksiköt ovat loogisia, toiminnallisia kytkentöjä ja yksiköitä; varsinaiset fyysiset kytkennät ja yksiköt voivat olla erilaiset. Alan ammattilaiselle on selvää, että järjestelmään voi kuulua muitakin elementtejä, yksiköitä, rakenteita ja/tai osajärjestelmiä, joita ei tarvitse kuvata tässä yksityiskohtaisemmin.

Kuvion 1A esimerkissä järjestelmä 100 käsittää transaktion lähtötiedon generoivana laitteena kassapäätteen 110, transaktiolla saatavan vastikkeen haluajan eli ostajan/maksajan/transaktion pyytäjän eli käyttäjän päätelaitteen 120, transaktion reaaliaikaisesti suorittavan järjestelmän (transaktion reaaliaikaisen suorittajan) eli pankkijärjestelmän 130, transaktiotietoja siirtävän siirtopalvelimen 140 ja tietoliikenneverkon 102, jonka välityksellä käyttäjän päätelaite, siirtopalvelin ja pankkijärjestelmä voivat kommunikoida.

Kassapääte 110 voi olla perinteinen kassapääte tai osa kassapäätejärjestelmää. Riittää, että kassapääte 110 käsittää laskunmuodostusyksikön (l-y) 111, jonka avulla se muodostaa käyttäjän ostoksista laskun. Lasku sisältää edullisesti vastikkeellisen transaktion vastineen (vastikkeesta halutun rahamäärän) eli maksettavan summan, ja saajan tietoja eli vastineen suorituskohteen eli ainakin yhden tai useamman tilinumeron, jolle maksun voi suorittaa, tai vastaavan tiedon, kuten vastaanottajan identifiointitieto, esimerkiksi Y-tunnus tai nimi, jolla tilitieto saadaan pankkijärjestelmässä selville. Jos myyjällä on useammassa eri pankissa tili, lasku voi sisältää kuhunkin pankkiin tilitiedot, tai myyjä voi valita laskuun tulevan pankin tai pankit. Myyjä voi esimerkiksi kysyä, minkä pankin tililtä ostaja aikoo maksaa ja valita laskuun tulevan tilitiedon sen perusteella. Lasku voi sisältää myös muuta tietoa, kuten viitenumeron. Lasku voi sisältää tai se voidaan esittää esimerkiksi yhtenä tai useampana viivakoodina ja/tai QR-koodina. Kassapääte voi myös käsittää yhden tai useamman rajapinnan (ei esitetty kuviossa 1) laskun tietojen ja/tai maksun suorittamisen välittämiseen. Eräs rajapinta voi olla NFC-moduuli, tai vastaava lyhyen kantaman tiedonsiirtomoduuli, jonka välityksellä lasku voidaan siirtää sähköisessä muodossa käyttäjän päätelaitteeseen 120, jos siinäkin on NFC-moduuli tai vastaava moduuli. Vaihtoehtoisesti tai sen lisäksi kassapääte voi käsittää rajapintana näyttölaitteen, jolla laskun tiedot voidaan näyttää ja/tai tulostimen,

jolla lasku tietoineen voidaan tulostaa. On myös mahdollista käyttää ohjelmointirajapintaa (API, Application Programming Interface), kuten OPOS (Object linking and embedding for retail Point Of Sale), joka mahdollistaa toiminnollisuuden/toiminnollisuuksien integroimisen suoraan kassapäätejärjestelmään ja siten kassapäätelaitteisiin. Toisin sanoen voidaan käyttää mitä tahansa tunnetun tekniikan tai tulevaisuuden kassapäätelaitetta, keksintö ei edellytä niihin mitään muutoksia. Joissakin suoritusmuodoissa myös kassapäätelaite ja/tai kassapäätejärjestelmä (osana taloushallintojärjesetlmää) voi olla konfiguroitu suorittamaan maksun vastaanottamiseen liittyviä toimintoja, kuten kuvioiden 4, 5A ja 5B yhteydessä kuvataan tarkemmin. Näissä suoritusmuodoissa laskunmuodostusyksikkö voi olla osa laskunhallintayksikköä.

Transaktion liipaisija (transaktion käynnistävä laite) eli käyttäjän päätelaite 120 on konfiguroitu olemaan tietoliikenneverkon 102 välityksellä yhteydessä transaktiotietoja siirtävän siirtopalvelimeen 140, ja siirtopalvelimen 140 kautta, tietoliikenneverkon 102 välityksellä, varsinaiseen transaktion suorittavaan järjestelmään eli kuvion 1A esimerkissä pankkijärjestelmään 130. Käyttäjän päätelaite voi olla matkaviestinlaite, esimerkiksi älypuhelin, tabletti, kannettava tietokone, kämmentietokone, älylasit, tai mikä tahansa puettava tietokone, älyvaate tai vastaava älylaite (laite, joka on mobiili ja sisältää laskentatehoa riippumatta siitä, mihin laite on asetettu). Käyttäjän päätelaite voi olla langallinen, kytkettävä tai langaton. Lisäksi päätelaite voi olla aktiivinen tai passiivinen. (Passiivinen laite, esimerkiksi ID-tagi, voidaan herättää käyntiin ja se voi saada käyttövirtansa toisesta laitteesta.) Päätelaitteen käyttöjärjestelmä voi olla mikä tahansa käyttöjärjestelmä (OS, operating system), kuten Android, iOS, Firefox OS, Windows Phone, BlackBerry 10, Tizen, Sailfish OS ja Ubuntu Touch. Toisin sanoen kuvion 1A esimerkissä kuluttajan päätelaite 120 voi olla mikä tahansa päätelaite, joka mahdollistaa yhteyden muodostamisen pankkijärjestelmään 130 yhden tai useamman tietoliikenneverkon 102 välityksellä siirtopalvelimen 140 kautta ja joka päätelaite 120 on konfiguroitavissa käynnistämään vastikkeellinen transaktio ja osallistumaan siihen. Sitä varten päätelaite käsittää yhden tai useamman rajapinnan (IFs) 123 ja suojatun osa-alueen 122, joka käsittää vastikkeellisen transaktion toteutusyksikön (v-t-t-y) 122-1, joka suoramaksusovelluksessa voi olla verkkopankkitoiminnan toteutusyksikkö, sekä tallentamisyksikön (t-y) 122-2 vastikkeellisessa transaktiossa tarvittavien tunnistetietojen tallentamiseksi suojattuun muistiin 122-3 ja suojatun muistin 122-3. Vastikkeellisen transaktion toteutusyksikön 122-1 toiminnolli-

suuksia kuvataan tarkemmin jäljempänä kuvioiden 2 – 4 yhteydessä. Tallentamisyksikkö 122-2 on konfiguroitu tallentamaan verkkopankkitoimintoa (tai mobiilipankkitoimintoa tai mitä tahansa reaaliaikaiseen sähköiseen maksamiseen tarkoitettua toimintoa) varten tarvittavat tunnusluvut, kuten verkkopankin kirjautumistunnukset ja mahdolliset avainluvut, tai osan tunnusluvuista suojattuna, kuten jäljempänä kerrotaan. Suojauksessa voidaan käyttää mitä tahansa salaustekniikkaa, kuten symmetristä tai epäsymmetristä salaustekniikkaa, tai sellaista hyödyntäviä tekniikoita, Apple-yhtiön kehittämää avainnippua (keychain) tai vastaavaa ratkaisua, tai täysin uusia ratkaisuja, kuten esimerkiksi salausavainkukkaroa, jota on kuvattu patenttihakemuksessa GB 1507154.1 Salausavainkukkaro, tai oikeastaan salausavainkukkaropari, on kahden osapuolen välinen salaus- ja salauksenpurkumekanismi, jossa kukkaro aukaistaan tunnisteella.

Suojattu osa-alue 122 on muista päätelaitteen sovelluksista eristetty, suojattu ympäristö, joka on tarkoitettu reaaliaikaisen transaktion toteuttavalle sovellukselle, niin että sovellus on suoritettavissa vasta, kun sovellus on varmistettu muuttumattomaksi ja käyttäjä tunnistettu, kuten myöhemmin kuvataan. Suojattu osa-alue voidaan toteuttaa käyttämällä esimerkiksi laitevalmistajan kehittämää ratkaisua. Eräs esimerkki tällaisesta on Samsung KNOX, joka eristää tiettyjä sovelluksia omalle alueelleen ja salaa eristetyn sovelluksen tiedot sekä lepotilassa että käytössä ollessa. Osa suojattua aluetta voidaan toteuttaa myös salaustekniikkaa käyttäen.

Suojattu osa-alue 122 käsittää suojatun muistin 122-3. Sen muuttamattomuus voidaan myös varmentaa ennen sovelluksen käynnistämistä tai sen yhteydessä, kuten myöhemmin kuvataan. Suojatussa muistissa 122-3 on suoramaksusovellusta varten erilaisia tunnistustietoja 122-31 ja mahdollisesti verkkopankkien tunnustietoja 122-32, joista ainakin osa, edullisesti kaikki salattuna, ja käytön aikana mahdollisesti osittain salauksesta purettuna.. Tällaisia tietoja ovat esimerkiksi julkisen avaimen hallintajärjestelmän (PKI, Public Key Infrastructure) yksityinen avain, sekä sovelluksen käytön edellyttämä tunnistustieto tai tiedot ja edullisesti myös siirtopalvelimen verkko-osoite. Esimerkiksi Samsung KNOX salaa suojatussa muistissa olevat tiedot käyttäen Advanced Encryption Standard (AES) –salausalgoritmia. Myös muita salausalgoritmeja, kuten esimerkiksi Salsa20 variantteineen voidaan käyttää. Tietojen käyttöä kuvataan tarkemmin jäljempänä kuvioiden 2-6 yhteydessä. Alan ammattilaiselle on ilmeistä, että tässä esitetty tallenta-

misjärjestely voidaan toteuttaa monilla eri tavoin, esimerkiksi osa tiedoista voidaan tallentaa yleiseen muistiin salattuna niin, että vain suojatulla alueella olevalla avaimella/avaimilla voidaan purkaa tietojen salaus.

Kuvion 1A esimerkissä vastikkeellisen transaktion suorittaja 130 on pankkijärjestelmä, joka mahdollistaa sähköisen reaaliaikaisen maksamisen tietoliikenneverkon 102 kautta tarjoamallaan sähköisellä maksurajapinnalla (maksurajapintayksikkö, m-y) 131, esimerkiksi verkkopankkisovelluksella tai mobiilipankkisovelluksella. Keksinnön mukaisissa ratkaisuissa voidaan käyttää mitä tahansa nykyistä tai tulevaisuuden pankkisovellusta eli käyttäjä voi vapaasti valita vastineen lähteen (mistä transaktion suoritetaan) eli asiointipankkinsa ja siellä tilinsä eikä keksintö vaadi muutoksia pankkien ratkaisuihin. Tulee myös huomata, että esimerkiksi erilaiset kanta-asiakastilit, joilla voi maksaa ostoksistaan, mahdollisesti jopa jollain muulla maksutavalla kuin rahalla, ovat tässä keksinnössä tasavertaisia vastineen lähteitä eli suoraan verrattavissa pankkitileihin; ne esimerkiksi näkyvät tileinä ja kanta-asiakasjärjestelmän tarjoaja voidaan vastaavasti tulkita yhdeksi verkkopankeista.

Kuvion 1A järjestelmässä transaktiotietoja siirtävä siirtopalvelin 140 on konfiguroitu siirtämään tietoliikenneverkon 102 välityksellä transaktiossa tarvittavia tietoja transaktion suorittavan järjestelmän 130 ja transaktion liipaisijan 120 välillä. Siirtopalvelin voi olla esimerkiksi sovelluspalvelin, joka yksinkertaisimmillaan on tietokone, joka suorittaa sovellusta. Toisin sanoen kuvion 1A esimerkissä siirtopalvelin 140 voi olla mikä tahansa tietokone, joka mahdollistaa suojatun yhteyden muodostamisen pankkijärjestelmään 130 ja päätelaitteeseen 120, ja joka on konfiguroitavissa osallistumaan vastikkeelliseen transaktioon. Sitä varten siirtopalvelin käsittää yhden tai useamman rajapinnan (IFs) 143, vastikkeellisen transaktion tietojensiirtoyksikön (v-t-t-s-y) 141, ja muistin ainakin 142 tunnistustietojen 142-1 ja eri verkkopankkien parsereiden (jäsentimien) 142-2 tallentamiseksi. Parserit esittävät tässä reaaliaikaisen suorittajan suorittajakohtaisia asetuksia. Pankkikohtaisilla parsereilla voidaan huomioida eri pankkien hiukan erilaiset verkkopankkitoteutukset, ja jopa maakohtaiset erot. Parserit voidaan toteuttaa millä tahansa tunnetulla tai tulevaisuuden parseritekniikalla. Esimerkiksi "Beatiful Soup" –nimellä kutsuttua Python-ohjelmointikielellä tehtyä parseripakettia voidaan käyttää. Verrattuna ratkaisuun, jossa tallennettaisiin esimerkiksi pankkien mobiilimaksusovellukset kokonaisuudessaan, tallentamalla pelkät parserit säästetään muistiresursseja. Lisäksi voidaan valita palvelimen käyttöjärjestelmä vapaasti; sovellukset tehdään aina jollekin käyttöjärjestelmälle, ja jos tallennettaisiin

mobiilimaksusovellukset, rajoittaisi se käyttöjärjestelmän valintaa. Myös käytettävyys on parempi. Vastikkeellisen transaktion tietojensiirtoyksikön 141 toiminnollisuutta kuvataan tarkemmin jäljempänä, erityisesti kuvioiden 3A-3B yhteydessä.

Kuviossa 1A esitetty tietoliikenneverkko 102 voi käsittää yhden tai useamman verkon, kukin verkko voi olla langaton verkko tai langallinen verkko tai niiden yhdistelmä. Sillä, miten tietoliikenneverkko on toteutettu, ei ole merkitystä keksinnölle. Tietoliikenneverkko tai osa siitä voi perustua esimerkiksi kolmannen, neljännen tai viidennen sukupolven langattomaan tietoliikenneteknologiaan, langattomaan lähiverkkoon, kuten Wi-Fi tai Li-Fi, tai muuhun langattomaan lähisiirtoon, kuten infrapuna, bluetooth, tai Internet-teknologiaan, laajakaistaverkkoteknologiaan ja/tai langalliseen puhelinverkkoon.

Suoritusmuodosta tai toteutustavasta riippuen se, mitä sovelluksen käytössä on tallennettu päätelaitteeseen 120, mitä siirtopalvelimeen 140 vaihtelee. Toisessa ääripäässä siirtopalvelimessa 140 on vain parserit, ja muu tieto on tallennettuna salattuna päätelaitteeseen 120 tai sitten päätelaite 120 on sovitettu pyytämään tietoja käyttäjältä, ja toisessa ääripäässä käyttäjän päätelaite 120 sisältää vain tiedot, joilla varmistetaan käyttäjän oikeus käyttää sovellusta, ja kaikki pankin käyttöön tarvittavat verkkotunnukset on tallennettu salattuna siirtopalvelimeen 140. Välimuotosovelluksissa esimerkiksi vakiona pysyvät tunnukset voidaan tallentaa salattuna siirtopalvelimeen ja kertakäyttöiset tunnukset salattuna päätelaitteen muistiin. Myös muita tapoja allokoida se, mitä tietoja on päätelaitteessa ja mitä siirtopalvelimessa, voidaan käyttää. On myös mahdollista, että samoja tietoja on tallennettu salattuna sekä siirtopalvelimeen että päätelaitteeseen.

Ratkaisu, jossa käytännössä kaikki tiedot ovat siirtopalvelimessa 140, vähentää verkon kuormitusta, kun tunnustietoja ei tarvitse kysyä ja siirtää. Toisaalta tunnustietojen tallentaminen käyttäjän päätelaitteeseen 120 lisää turvallisuutta: yhden henkilön tietoja sisältävän yksittäisen päätelaitteen hakkerointi on vähemmän kiinnostavaa kuin usean henkilön tietoja sisältävän palvelimen, sillä yksittäisen ihmisen verkkotunnusten hakkeroinnilla mahdollisesti saavutettava hyöty jää selvästi pienemmäksi.

Tallentamisyksikkö 122-2 on sovitettu tallentamaan verkkopankkien tunnustiedot 122-32 edullisesti verkkopankkikohtaisesti ja toteutusmuodosta riippuen salattuna joko osissa tai kokonaisuutena. Tallentamisyksikkö voi tallentaa tiedot paitsi päätelaitteeseen 120 myös siirtopalvelimeen 140. Tallentamisyksikkö 122-2 edullisesti salaa tallennettavat tiedot. Tietojen salaamiseen voidaan käyttää

mitä tahansa salaustekniikkaa. Tallennettavat vakiotiedot salataan edullisesti käyttäen eri salausavainta tai –avaimia kuin mitä käytetään muuttuvien tietojen salaamiseen. Näin mahdollisesti tunnettu tieto ei vaaranna koko suojaa. Tallentamisyksikkö 122-2 voi olla konfiguroitu salaamaan päätelaitteeseen tallennettavat tiedot niin, että ne ovat purettavissa vain siirtopalvelimen salauksenpurkuavaimella. Päätelaitteessa ja siirtopalvelimessa voi olla myös salausavainkukkarot (kukkaropari), jonka avulla tiedot voidaan salata.

Esimerkiksi salausavainkukkaroa käytettäessä tunnukset voidaan tallentaa kukkaroon niin että kukkaron auki ollessa ne kaikki ovat luettavissa esimerkiksi avaimen sarjanumeron perusteella. Tunnukset voidaan tallentaa myös yksittäin salattuna, esimerkiksi niin ettei sen avaimen sarjanumeroa tallenneta. Näin saadun osoiteavaruuden avulla salatut tunnukset löytyvät, ja jos ne on tallennettu päätelaitteeseen, ne ovat siirrettävissä salaustavasta riippuen salattuna päätelaitteesta siirtopalvelimeen tai yksittäin salauksesta purettuna. Kun tiedot ovat erikseen salattuna, siirtopalvelimen tietoturvallisuus paranee, sillä sielläkin tiedot pitää hakkeroida yksitellen ja lisäksi auki saadut tiedot pitää osata yhdistää oikeisiin tileihin.

Päätelaitteen tallentamisyksikkö 122-2 voi saada tiedot, kuten avainlukulistan esimerkiksi niin että käyttäjä syöttää tiedot, käyttää päätelaitteen QR-skanneria tai muuta vastaavaa skanneria, valokuvaa tunnukset, saa ne sähköisesti pankista yms.

Paitsi päätelaitteen 120 kautta siirtopalvelin 140 voi saada tiedot myös suoraan pankista 130.

Tulee myös huomata, että tulevaisuudessa myös pankkiyhteys voi toimia salausavainkukkaron kanssa ja tällöin sen (käyttäjäkohtainen) vastinpari joko siirtopalvelimessa tai päätelaitteessa voi korvata käyttäjäkohtaiset pankkitiedot. Siirtopalvelinta käyttävässä ratkaisussa voi siten siirtopalvelimessa olla kaksi avainkukkaron vastinparia samalle käyttäjälle – toinen siirtopalvelimen ja päätelaitteen välillä käytettäväksi ja toinen siirtopalvelimen ja pankin välillä käytettäväksi. On myös mahdollista, että joskus tulevaisuudessa siirtopalvelimen ja pankin välillä käytetään, luonnollisesti käyttäjien suostumuksella, yhtä salausavainkukkaroparia (käyttäjille yhteistä salausavainkukkaroparia) pankin ja siirtopalvelimen välille kaikille suostumuksensa antaneille käyttäjille. Salausavainkukkaroilla voi olla tunnisteen lisäksi myös sarjanumero, jonka perusteella tunnistetaan, mikä salausavainkukkaro milloinkin on käytössä. Avainkukkaron sarjanumero voidaan pi-

tää erillisenä avaimen sarjanumerosta, mutta sarjanumerot voidaan myös haluttaessa yhdistää. On myös mahdollista, että samaa salausavainkukkaroa käytetään myös ryhmälle eri osapuolia (eli ryhmällä on yhteinen salaisuus). Salausavainkukkarolla on siten mahdollista saavuttaa sama kuin sovellettaessa Diffie-Hellman-avaimenvaihtoprotokollaa usean osapuolen kesken, paitsi että salausavainkukkaroa käytettäessä salauksen prosessi ei hidastu, kuten pelkästään Diffie-Hellman-avaimenvaihtoprotokollaa käytettäessä käy.

Kuvion 1B esimerkkijärjestelmä 100 eroaa kuvion 1A esimerkkijärjestelmästä siinä, että erillistä siirtopalvelinta ei ole, vaan käyttäjän päätelaite 120a on konfiguroitu suorittamaan myös tiedonsiirron suoraan vastikkeellisen transaktion suorittajan eli pankkijärjestelmän 130 kanssa. Sitä varten käyttäjän päätelaite 120a käsittää laajennetun vastikkeellisen transaktion toteutusyksikön (l-v-t-t-y) 122-1a, joka on yhdistelmä kuvion 1A esimerkin vastikkeellisen transaktion toteutusyksiköstä ja vastikkeellisen transaktion tietojensiirtoyksiköstä, sekä muistissa, joko suojatussa muistissa 122, kuten kuviossa 1B, tai suojaamattomassa muistissa, eri verkkopankkien parserit 123-33. Toteutustavasta riippuen muistissa voi olla kaikkien verkkopankkien, mukaan lukien kanta-asiakasjärjestelmät, parserit tai vain niiden verkkopankkien parserit, joiden tileiltä käyttäjä voi vastikkeellisen transaktion suorittaa eli maksaa. Jälkimmäinen ratkaisu kuluttaa vähemmän muistiresursseja.

Siirtopalvelinta käytettäessä etuna on se, että kun pankki (tai kanta-asiakasjärjestelmä) muuttaa verkkopankkitoiminnollisuuttaan, on parserin päivittäminen vastaavasti yksinkertaista: parseri täytyy päivittää vain siirtopalvelimeen. Siirtopalvelittomassa ratkaisussa parsereiden päivittäminen kuormittaa enemmän resursseja, sillä parseri täytyy päivittää jokaiseen päätelaitteeseen, jossa se on. Sitä varten täytyy jossain ylläpitää tietoa päätelaitteista, ja jos päätelaitteeseen tallennettujen parsereiden määrä vaihtelee päätelaitteittain, täytyy ylläpitää tietoa mitä parsereita missäkin päätelaitteessa on tai vaihtoehtoisesti kysyä aina päivityksen yhteydessä päätelaitteilta, mitä parsereita niillä on.

Kuviossa 2 esitetään eräs esimerkki, yhdessä kuvioiden 7A-7C kanssa, vastikkeellisen transaktion toteutusyksikön toiminnasta, joka tässä esimerkissä on siirtopalvelinta käyttävä reaaliaikainen maksusovellus. Tulee ymmärtää, että vastikkeellinen transaktion toteutusyksikkö voidaan jakaa aliyksiköihin, jotka suorittavat tietyt, jonkun osakokonaisuuden muodostavan osuuden, toiminnot. Kuvion 2 esimerkissä oletetaan, että sovelluksen varmentaminen, muistin varmentaminen

ja käyttäjän tunnistautuminen onnistuvat. Jos joku niistä ei onnistu, prosessi luonnollisesti keskeytyy.

Viitaten kuvioon 2, kun maksusovelluksen käynnistäminen havaitaan vaiheessa 200, maksusovellus varmennetaan (todennetaan) vaiheessa 200. Tähän vaiheeseen voi kuulua myös maksusovelluksen tunnistaminen esimerkiksi julkisen avaimen hallintajärjestelmän avulla. Käynnistämisen voi liipaista laskun vastaanottaminen sähköisesti kassapäätelaitteelta tai käyttäjän syöte (valinta), joka käynnistää sovelluksen. Käyttäjä voi esimerkiksi valita, kuten kuviossa 7A on esitetty, sovelluksen (MAKSAJA) 50 päätelaitteensa yleisnäytöllä 500. Maksusovelluksen varmentaminen voidaan tehdä esimerkiksi laskemalla maksusovelluksesta sen tarkistussumma tai tarkisteavain, joka on luotu esimerkiksi CRC:llä (Cyclic redundancy check), tai kryptografisella tiivisteellä, joka on luotu esimerkiksi jollain SHA-funktiolla (SHA, Secure Hash Algorithm), kuten SHA-1, SHA-2, tai edullisesti SHA-3, ja vertaamalla laskutulosta tunnistustiedoissa olevaan sovelluksen tarkistussummaan tai tarkisteavaimeen tai tiivisteeseen. Jos ne ovat samat, on sovellus muuttumaton eli varmennettu. Toisin sanoen käytännössä varmistetaan, että sovelluksen koodia ei ole muutettu, ja että sovellus on ladattu tunnistetulta ja luotetulta taholta. Tässä esimerkissä myös varmennetaan muisti vaiheessa 201. Muisti voidaan varmentaa samalla tavalla kuin sovellus. Tyypillisesti laitteen valmistaja on määritellyt muistinvarmistamistavan. Sen jälkeen suoritetaan käyttäjän tunnistautuminen vaiheessa 201. Käyttäjä voidaan tunnistaa esimerkiksi päätelaitteeseen integroidun biometrisen tunnistimen avulla, kuten PositiveID, sormenjälkitunnistin tai iiristunnistin, mahdollisesti kaksivaiheisena tunnistuksena, jossa biometrinen tunnistaminen on yhdistetty käyttäjän salasanaan tai päätelaitteen PIN-koodiin/ turvakoodiin ja/tai päätelaitteen avaavaan suojakoodiin. Biometrisen tunnistimen tilalla tai sen kanssa yhdessä voidaan käyttää mitä tahansa digitaalista kredentiaalia. Yksi turvallinen vaihtoehto on käyttäjän päätelaitteen käyttöönotossa yhdistää päätelaitteeseen integroitu sormenjälkitunnistus tai muu vahva tunnistautuminen toista ulkoista reittiä välitettyyn tietoon, kuten NFC- lukijan tai RFID- lukijan kautta välitettyyn fyysisestä sormuksesta, kellosta, implantista tai avaimenperästä saatuun tietoon. Sovelluksen tallentamisella suojattuun muistiin ja vahvalla käyttäjän tunnistuksella ennaltaehkäistään mahdollisia haitta- tai vakoiluohjelmien aiheuttamia tietovuoto-ongelmia.

Kun käyttäjä on tunnistettu, eli on varmistettu hänen oikeutensa käyttää tilejä, luetaan vaiheessa 202 kassapäätteeltä lasku eli maksettava summa ja tieto tilistä tai tileistä, joihin maksaminen voidaan suorittaa. Myös muuta tietoa,

20165360 PRH 26-08-2016

kuten viitenumero tai arkistointitunnus, voidaan välittää. Lukeminen voidaan suorittaa mitä tahansa tunnettua tekniikkaa käyttäen. Lukeminen voidaan suorittaa käyttäen esimerkiksi NFC-lukijaa tai muuta vastaavaa lyhyen kantaman lukijaa, kuten infrapuna tai wi-fi tai valo, käyttäen, lukemalla päätelaitteen sovellusta ja kameraa hyödyntäen QR-koodi (t) ja/tai viivakoodi(t). Lasku eli maksu voidaan lukea myös värinätunnistetta käyttäen värinän avulla tai äänitunnistusta käyttäen äänen avulla. Tässä esimerkissä laskun lukemiseksi katsotaan myös laskutietojen manuaalinen syöttö päätelaitteen käyttöliittymän välityksellä. Tieto voidaan siirtää myös kiinteää väylää pitkin esimerkiksi USB-liitännän välityksellä.

Kun lasku on luettu, muutetaan se tarvittaessa vaiheessa 203 maksuksi. Luonnollisesti, jos luettava lasku on suoraan maksumuotoinen, muotoilua ei tarvitse suorittaa.

Samanaikaisesti, tai sen jälkeen määritellään vaiheessa 204 käyttäjän käytössä olevat tilit sekä maksussa olevat pankit. Luonnollisesti käyttäjän käytössä olevat tilit on voitu määritellä jo aiemmin, esimerkiksi lukea niiden tiedot käynnistämisen yhteydessä suojatusta muistista. Jos käyttäjällä on käytössään useampi tili kuin yksi (vaihe 205: kyllä), pyydetään käyttäjää valitsemaan tili, jota hän haluaa käyttää. Eräässä toisessa suoritusmuodossa, jos laskussa on useampi kuin yksi pankki, pyydetään käyttäjää valitsemaan myös pankkitili, jolle hän haluaa maksaa, olipa käyttäjällä kuinka monta tiliä tahansa. Käyttäjää pyydetään valitsemaan tili näyttämällä pyyntö ja tilivaihtoehdot päätelaitteen näytöllä, tai näyttämällä pelkät tilit. Suoritusmuodosta riippuen tilit voidaan näyttää aina samassa järjestyksessä, siinä järjestyksessä, jossa niitä on eniten käytetty, pankkikohtaisessa järjestyksessä (jos samaan pankkiin on useampi tili) ja/tai järjestyksessä voidaan huomioida maksussa oleva pankki/olevat pankit niin, että ylimmäisenä ovat tilit, jotka ovat samassa pankissa kuin mitä on maksussa, esimerkiksi maksussa olevassa järjestyksessä. Eräs esimerkki on esitetty kuviossa 7B, jossa käyttäjän päätelaitteen käyttöliittymän sovellusnäytöllä 501 näytetään tilivalinnat 51. Kuvion 7B esimerkissä käyttäjällä on kaksi tiliä pankissa P3, yksi tili pankissa P1 ja yksi tili pankissa P2. Tulee ymmärtää, että edellä on esitetty vain muutama esimerkki siitä, millä perusteella ja miten tilejä voi näyttää käyttäjälle. Kun käyttäjän tilivalinta vastaanotetaan vaiheessa 207, näytetään maksutapahtuma sen jälkeen vaiheessa 208 käyttäjälle yhdessä maksun hyväksyntäpyynnön eli vahvistuspyynnön kanssa. Eräs esimerkki on esitetty kuviossa 7C, jossa käyttäjän päätelaitteen käyttöliittymän sovellusnäytöllä 701 näytetään maksutapahtuma 72 eli summa ja tili, jolta

20165360 PRH 26-08-2016

summa veloitetaan sekä valintanäppäimet 72a, 72b, joiden avulla käyttäjä voi hyväksyä tai hylätä maksun. Toisin sanoen tässä vaiheessa vielä varmistetaan, että käyttäjä haluaa maksaa laskun. Jos vaihtoehtoja ei ollut (vaihe 205: ei), saavutaan suoraan tähän vaiheeseen. Jos käyttäjä ei hyväksy maksua (vaihe 209:ei), maksaminen ja sovellus keskeytetään vaiheessa 216.

Jos käyttäjä hyväksyy maksun (vaihe 209: kyllä) suoritetaan verkkomaksu. Verkkomaksun suorittaminen aloitetaan muodostamalla vaiheessa 210 suojattu yhteys siirtopalvelimeen, esimerkiksi HTTPS-yhteys (HTTPS, Hypertext Transfer Protocol Secure), jossa HTTP-tiedonsiirtoprotokollaa käytetään joko TLS (Transport Layer Security) tai SSL (Secure Sockets Layer) salausprotokollan kanssa. Jälkimmäisen käyttö edellyttää, että osapuolet luottavat toistensa SSL-sertifikaattiin. Suojattu yhteys voidaan muodostaa myös muulla tavoin, kuten edellä mainittua salausavainkukkaroa hyödyntäen. On myös mahdollista suojatun yhteyden lisäksi välittää tiedot suojattuna/salattuna, esimerkiksi OpenPGP standardin mukaisella PGP:llä (Pretty Good Privacy). Jos tiedot on salattu niin, että vain siirtopalvelin saa salauksen purettua, voidaan tiedot lähettää jopa normaalilla tiedonsiirtoyhteydellä.

Kun suojattu yhteys on muodostettu, lähetetään vaiheessa 211 maksamiseen liittyvät tiedot eli tili, josta maksetaan, tili, jolle maksetaan, ja summa, joka maksetaan siirtopalvelimelle. Toisin sanoen esimerkiksi maksajan tilitietoa ei missään vaiheessa siirretä kassapäätelaitteelle, joten riski tietojen joutumiselle väärin käsiin on pienempi ja kassapäätejärjestelmältä ei näin ollen vaadita niin suurta turvallisuutta kuin esimerkiksi pankkikortti- ja luottokorttimaksuissa.

Kun siirtopalvelimelta vastaanotetaan viesti (vaihe 212), tarkistetaan vaiheessa 213, onko se maksamiseen liittyvien tietojen pyyntö vai ei. Esimerkkejä eri tietopyynnöistä esitetään kuvioissa 3A ja 3B. Jos kyseessä oli pyyntö (vaihe 213:kyllä), haetaan vaiheessa 214 verkkopankkitunnuksista, joiden salaus on tausta-ajona purettu, pyydetyt tiedot ja lähetetään vaiheessa 214 ne, jonka jälkeen palataan vaiheeseen 212 vastaanottamaan viestiä siirtopalvelimelta.

Jos kyseessä ei ollut pyyntö (vaihe 213: ei), saadaan tieto maksutapahtuman onnistumisesta, ja näytetään se vaiheessa 215. Jos maksu onnistui, tieto on edullisesti kuitti maksusta tai katevarauksen osoittava tieto maksusta, ja kun se näkyy näytöllä, voidaan se näyttää myyjälle ja saada vastike eli tavara tai tavarat, jotka oli ostettu. Tämän jälkeen sovellus voi sulkeutua automaattisesti tai se voi odottaa käyttäjältä "sulje" –syötettä ja/tai tarjota käyttäjälle mahdollisuuden suorittaa uusi maksu. Sovellus voi myös olla järjestetty tunnistamaan epäonnistunut

20165360 PRH 26-08-2016

maksu, mahdollisesti myös epäonnistumisen syy, kuten esimerkiksi väärä tunnus/tunniste tai se, että tilillä ei ollut tarpeeksi rahaa. Jos käyttäjällä on useampia eri tilejä, voidaan palata vaiheeseen 206, ja esimerkiksi näyttämään sillä kertaa tilit, joilta ei vielä ole yritetty maksaa.

Kuvioissa 3A ja 3B kuvataan yksityiskohtaisemmin varsinaiseen verkkomaksamiseen liittyvää tiedonsiirtoa käyttäjän päätelaitteen (vastikkeellisen transaktion toteutusyksikön), siirtopalvelimen (vastikkeellisen transaktion tietojensiirtoyksikön), verkkopankin (verkkopankkijärjestelmän eli vastikkeellisen transaktion reaaliaikaisen suorittajan) ja vastaanottajan (vastaanottajan tilijärjestelmän) välillä. Kuvioissa 3A ja 3B oletetaan, että maksaminen onnistuu. Lisäksi kuvioissa suojatulla yhteydellä lähetetyt tiedot salataan ennen lähettämistä ja puretaan ennen käyttämistä, mutta selvyyden vuoksi salaamista ja vastaavasti salauksen purkamista ei toisteta tietojen vaihtamisen yhteydessä. Luonnollisesti, jos esimerkiksi joku tunniste tai haaste-vastepari on väärä, maksaminen epäonnistuu. Tulee ymmärtää, että jossain suoritusmuodossa voidaan tunnistetta tai haaste-vasteparia kysyä uudelleen esimerkiksi kerran, kaksi kertaa tai kolme kertaa ennen kuin maksaminen epäonnistuu.

Viitaten kuvioon 3A, kun käyttäjän päätelaitteessa on suoritettu (kohta 3-1) sovelluksen eli vastikkeellisen transaktion toteutusyksikön varmentaminen, käyttäjän tunnistaminen, ja maksamiseen liittyvät vaiheet aina siihen asti, että maksu on hyväksytty eli ollaan kuvion 2 vaiheen 209:kyllä jälkeisessä tilanteessa. Sen jälkeen muodostetaan suojattu yhteys (viestit 3-2) päätelaitteen ja siirtopalvelimen välille. Kuten kuvion 2 yhteydessä on kerrottu, yhteys voi olla HTTPS-yhteys, jossa tiedot salataan ennen lähettämistä esimerkiksi TLS-protokollalla. Kun yhteys on saatu muodostettua, lähetetään (viesti 3-3) maksamiseen liittyvät tiedot eli maksajan tili, myyjän tili ja summa.

Vastaanotettuaan maksamiseen liittyvät tiedot, määrittelee siirtopalvelin maksajan tilin perusteella maksajan pankin ja valitsee kohdassa 3-4 käytettävän parserin sekä muodostaa suojatun yhteyden (viestit 3-5, 3-6), esimerkiksi HTTPS-yhteyden, pankin verkkopankkiin tietojen vaihtamista varten.

Sen jälkeen suoritetaan varsinainen verkkopankkiyhteyden muodostaminen verkkopankkiin kirjautumisineen suojattuja yhteyksiä käyttäen.

Ensiksi siirtopalvelin pyytää (viesti 3-7) verkkopankilta sen sisäänkirjautumissivun (www-sivu, tai URL (uniform resource locator)) hypertekstin merkintäkielisen (HTML) sisällön ja saatuaan viestissä 3-8 verkkopankin palauttaman sisällön, käynnistää valitun pankkikohtaisen parserin ja etsii kohdassa 3-9 parserin

avulla kirjautumiseen vaadittavien input-elementtien kentät. Tyypillisesti kentät ovat pankkikohtaisesti kirjautumiseen määritetyssä HTML form –element lomakkeessa. Ne löydettyään siirtopalvelin pyytää vaadittavat tiedot (viesti 3-10) käyttäjän päätelaitteelta.

Käyttäjän päätelaite hakee (kohta 3-11) valitun tilin pankin verkkopankin tunnustiedoista pyydetyt tiedot ja palauttaa ne siirtopalvelimelle viestissä 3-12. Mikäli tiedot on tallennettu osissa, voi käyttäjän päätelaite purkaa nämä tiedot sisältävän osan suojauksen joko tässä vaiheessa, tai jos tiedot on suojattu pankkikohtaisena kokonaisuutena, kaikki tiedot. Vaihtoehtoisesti tietojen suojaus voidaan purkaa jo aikaisemmin tausta-ajona esimerkiksi vasteena maksun hyväksymiselle. Toteutusmuodosta riippuen myös käyttäjältä voidaan kysyä näitä kirjautumistietoja, tai ainakin yhtä niistä, jos kirjautumistietoja tarvitaan useampi.

Saatuaan kirjautumistiedot siirtopalvelin koostaa kohdassa 3-13 vastauksen. Toisin sanoen tässä esimerkissä se koostaa input-elementtien kentät HTTP POST –pyynnöksi (request) ja lähettää ne (viesti 3-14) viestissä 3-8 saatuun URL-osoitteeseen. (Kuvion esimerkissä URL-osoite on kirjautumislomakkeen form-elementin action-attribuutissa.) Kuvion esimerkissä oletetaan, että kirjautumistiedot olivat oikeat, joten kun siirtopalvelimen parseri lukee verkkopankin palauttaman vastineen (viesti 3-15) eli HTML-sisällön, toteaa se kohdassa 3-16 olevansa kirjautunut verkkopankkiin.

Kirjautumisen jälkeen suoritetaan verkkopankki-istunnon aktivointi.

Ensiksi siirtopalvelin pyytää (viesti 3-17) verkkopankilta sen istunnon aktivointilomakkeen HTML-sisällön ja saatuaan viestissä 3-18 verkkopankin palauttaman sisällön, parseri etsii kohdassa 3-19 haastevasteluvun haastekoodin, esimerkiksi aktivointilomakkeen form-elementin tai input-elementin, ja pyytää (viesti 3-20) haastekoodia käyttäjän päätelaitteelta.

Käyttäjän päätelaite hakee (kohta 3-21) valitun tilin pankin verkkopankin tunnustiedoista haastekoodin ja palauttaa sen siirtopalvelimelle viestissä 3-22. Mikäli tiedot on tallennettu osissa, voi käyttäjän päätelaite purkaa tämän tiedon sisältävän osan suojauksen tässä vaiheessa. Toteutustavasta riippuen haastekoodi voidaan vaihtoehtoisesti pyytää myös käyttäjältä.

Saatuaan haastekoodin siirtopalvelin koostaa kohdassa 3-23 vastauksen. Toisin sanoen tässä esimerkissä se koostaa input-elementtien kentät HTTP POST –pyynnöksi (request) ja lähettää (viesti 3-24) täytetyn haastevastekoodin input –elementin kentät viestissä 3-18 saatuun URL-osoitteeseen. (Kuvion esimer-

kissä URL-osoite on haastevastelukulomakkeen form-elementin action-attribuutissa.) Kuvion esimerkissä oletetaan, että haastevastekoodi oli oikea, joten kun siirtopalvelimen parseri lukee verkkopankin palauttaman vastineen (viesti 3-25) eli HTML-sisällön, toteaa se kohdassa 3-26 verkkopankki-istunnon olevan aktivoitu.

Sen jälkeen suoritetaan maksun kirjaus.

Ensiksi siirtopalvelin pyytää (viesti 3-27) verkkopankilta sen laskunmaksulomakkeen HTML-sisällön ja saatuaan viestissä 3-28 verkkopankin palauttaman sisällön, parseri etsii ja täyttää, viestissä 3-3 vastaanotettuja tietoja käyttäen, kohdassa 3-29 maksamiseen vaaditut input-elementit, esimerkiksi tilinumero, jolta maksu veloitetaan, laskun saajan nimi, laskun viitenumero, laskun summa ja saajan tilinumero. Osa input-elementeistä voi olla pakollisia ja osa vapaaehtoisia. Toteutustavasta riippuen siirtopalvelin voi pyytää käyttäjälaitteelta tai sen välityksellä maksajalta mahdollisesti puuttuvia tietoja. Kun maksamisessa tarvittavien input-elementtien tiedot on selvitetty, siirtopalvelin koostaa kohdassa 3-29 maksun. Toisin sanoen tässä esimerkissä se koostaa input-elementtien kentät HTTP POST –pyynnöksi (request) ja lähettää (viesti 3-30) täytetyn laskunmaksulomakkeen viestissä 3-28 saatuun URL-osoitteeseen. (Kuvion esimerkissä URL-osoite on haastevastelukulomakkeen form-elementin action-attribuutissa.)

Kuvion 3A esimerkissä oletetaan, että tilillä oli rahaa, joten verkkopankki suorittaa alustavan maksamisen (maksuvarauksen kirjaamisen) kohdassa 3-31 ja palauttaa siitä vastineen (viesti 3-32).

Kun siirtopalvelimen parseri lukee verkkopankin palauttaman vastineen (viesti 3-32) eli HTML-sisällön, se havaitsee, että maksun kirjaus on tehty.

Maksun kirjauksen jälkeen siirtopalvelin, oikeammin siirtopalvelimen parseri, käynnistää siksi maksun vahvistuksen ja hyväksymisen.

Ensiksi siirtopalvelin pyytää (viesti 3-33) verkkopankilta sen maksun vahvistuslomakkeen HTML-sisällön ja saa viestissä 3-34 verkkopankin palauttaman sisällön.

Sen jälkeen kuvion 3A prosessi jatkuu kuviossa 3B.

Sisällön (viesti 3-34) saatuaan parseri etsii kohdassa 3-35 sisällöstä haastevasteluvun haastekoodin, esimerkiksi haastevastelomakkeen form-elementin tai input-elementin, ja pyytää (viesti 3-36) haastekoodia käyttäjän päätelaitteelta.

Käyttäjän päätelaite hakee (kohta 3-37) valitun tilin pankin verkkopankin tunnustiedoista haastekoodin ja palauttaa sen siirtopalvelimelle viestissä

3-38. Mikäli tiedot on tallennettu osissa, voi käyttäjän päätelaite purkaa tämän tiedon sisältävän osan suojauksen tässä vaiheessa. Toteutustavasta riippuen haastekoodi voidaan vaihtoehtoisesti pyytää myös käyttäjältä.

Saatuaan haastekoodin siirtopalvelin koostaa kohdassa 3-39 vastauksen. Toisin sanoen tässä esimerkissä se koostaa input-elementtien kentät HTTP POST –pyynnöksi (request) ja lähettää (viesti 3-40) täytetyn haastevastekoodin input –elementin kentät viestissä 3-34 saatuun URL-osoitteeseen. (Kuvion esimerkissä URL-osoite on haastevastelukulomakkeen form-elementin action-attribuutissa.) Kuvion esimerkissä oletetaan, että haastevastekoodi oli oikea, joten verkkopankki suorittaa kohdassa 3-41 maksun ja palauttaa siitä siirtopalvelimelle tiedon (viesti 3-42). Samalla tieto maksusta siirtyy (viesti 3-43) normaalin verkkopankissa tapahtuvan maksun tapaan myös vastaanottajan pankkijärjestelmään reaaliaikaisesti. Näin tieto maksusta saadaan tarvittaessa myös lain vaatimaan fiskaalijärjestelmään ja siten myös paikalliselle verottajalle. Tämä tarkoittaa sitä, että jos tilit ovat samassa pankissa tieto maksusta (kohta 3-52) vastaanotetaan käytännössä välittömästi, mutta toistaiseksi eri pankkien välillä voi olla viivettä.

Kun siirtopalvelimen parseri lukee verkkopankin palauttaman vastineen (viesti 3-42) eli HTML-sisällön, toteaa se kohdassa 3-44 maksun maksetuksi.

Sen jälkeen suoritetaan vielä maksun todennus.

Ensiksi siirtopalvelin pyytää (viesti 3-45) verkkopankilta maksetun laskun kuitin HTML-sisällön ja saatuaan viestissä 3-46 verkkopankin palauttaman sisällön, parseri etsii siitä arkistointitunnuksen ja koostaa sitä käyttäen kohdassa 3-47 kuitin, jonka lähettää (viesti 3-48) käyttäjän päätelaitteelle. Tässä esimerkissä käyttäjän päätelaite on sovitettu näyttämään kohdassa 3-49 kuitti päätelaitteen näytössä. Jossain muussa toteutusmuodossa kuitti voidaan lähettää sen sijaan tai sen lisäksi kassapäätteelle, joka, jos se on konfiguroitu, voi vahvistaa kassapäätteen käyttäjälle, että maksu on suoritettu.

Kuvion 3B esimerkissä maksun todentamisen jälkeen lopetetaan verkkopankki-istunto siirtopalvelimen ja verkkopankin välillä (viestit 3-50) ja suojattu yhteys siirtopalvelimen ja käyttäjän päätelaitteen välillä (viestit 3-51).

Suoritusmuodoissa, joissa verkkopankkien tunnukset on tallennettu salattuna siirtopalvelimeen, viestissä 3-3 voidaan välittää tietoa, jonka avulla verkkopankkien tunnusten salaus voidaan purkaa. Esimerkiksi voidaan toimittaa yhteinen jaettu salaisuus tai julkisen avaimen vastinparina salainen avain. Erittäin tietoturvallinen tapa on myös toimittaa salausavainkukkaron avaava tunniste. Salauksen purkamisessa tarvittavan tiedon välittäminen voi myös sisältää useamman

20165360 PRH 26-08-2016

viestin lähettämisen siirtopalvelimen ja päätelaitteen välillä. Suoritusmuodoissa, joissa tiedot on tallennettu siirtopalvelimeen, viestit 3-10, 3-12, 3-20, 3-22, 3-36, ja 3-38 ovat siirtopalvelimen sisäistä tiedonsiirtoa ja kohdat 3-11, 3-21 ja 3-37 suoritetaan siirtopalvelimessa. Suoritusmuodoissa, joissa osa tiedoista on siirtopalvelimessa ja osa päätelaitteessa, osa kuvion 3 yhteydessä kuvatuista viesteistä voi olla siirtopalvelimen sisäistä tiedonsiirtoa (ja vastaavat kohdat suoritetaan siirtopalvelimessa).

On myös mahdollista, että maksun vastaanottaja, kuten kauppias, vaatii sähköisesti allekirjoitettua kuittia suoritetusta maksusta. Sähköiseen allekirjoitukseen voidaan käyttää mitä tahansa tunnettua tai tulevaisuuden tekniikkaa, kuten käyttäen henkilökohtaisia pankkitunnuksia sähköiseen allekirjoitukseen tai Signom-allekirjoituspalvelua.

Suoritusmuodoissa, joissa ei käytetä siirtopalvelinta, kuvioissa 3A ja 3B esitetty siirtopalvelimen ja päätelaitteen välinen tiedonsiirto on päätelaitteen, tai oikeammin laajennetun vastikkeellisen transaktion toteutusyksikön suorittamaa, sisäistä tiedonsiirtoa.

Kuten edellä olevista esimerkeistä selviää, sovellus toimii ikään kuin parannettuna, esimerkiksi turvallisuudeltaan varmempana digitaalisena pankkikorttina – maksetaan suoraan omalta tililtä lähettämättä tietoja tilistä, ja käyttäjän oikeus käyttää sovellusta varmennetaan tehokkaammin kuin perinteisen pankkikortin tapauksessa, jossa varmennus perustuu lyhyeen PIN-koodiin.

Edellä esitetyissä esimerkeissä on oletettu, että käytetään tunnetun tekniikan mukaista kassapäätejärjestelmää eikä siihen ole tehty muutoksia. Tällaisten suoritusmuotojen etuna on, että koska maksajan ja maksun saajan laitteiden ei tarvitse tukea samaa sovellusta, käyttökohteita ei ole rajoitettu eikä laajan kattavuuden saamiseksi laitteistojen tarvitse tukea useaa eri sovellusta. Niissä myös vältetään päätelaitteissa toimivien sovellusten, jotka mahdollistavat pankin mobiilimaksusovelluksen käyttämisen, laskun maksuun, jos lasku on toimitettu samalla sovelluksella, joka käynnistää pankin mobiilimaksusovelluksen, ongelmat: maksajan täytyy joko etukäteen siirtää rahaa päätelaitteeseensa tai rekisteröityä samaan, maksun saajalle maksuja välittävään palveluun kuin maksun saaja.

Edellä esitettyjä esimerkkejä voidaan soveltaa myös, kun kassapäätejärjestelmään tehdään muutos, jolla varmistetaan reaaliaikaisesti, että maksu on suoritettu myös silloin, kun saajan pankki on eri kuin maksajan pankki. Näissäkin, kuvioiden 4, 5A ja 5B esimerkkien avulla esitetyissä suoritusmuodoissa, vältetään

edellä esitetyt ongelmat, sillä yhdellä sovelluksella katetaan kaikki pankit eli saadaan laaja kattavuus, rahaa ei tarvitse siirtää etukäteen eikä erillistä rekisteröitymistä tarvita. Tulee huomata, että asiakkaan päätelaitteessa olevan sovelluksen ei välttämättä tarvitse olla sama sovellus kuin kassapäätejärjestelmässä oleva sovellus (tai sovellusparin vastinpari), vaan riittää, että sovelluksilla on riittävästi yhtenäisiä toiminteita jäljempänä kuvattujen toiminteiden varmistamiseen.

Kuvioiden 4, 5A ja 5B esimerkeissä esitetään laskunhallintayksikön (tai yksiköiden) toiminnollisuutta. Kuvion 4 esimerkissä oletetaan, että varmennus pyydetään aina ja kuvioiden 5A ja 5B esimerkissä oletetaan, että varmennus pyydetään vain, jos oman pankin kautta ei saada reaaliajassa tietoa. Kuviossa 4 on selitetty myös sitä, kuinka esimerkiksi parseri tai käyttäjän päätelaitteen tai siirtopalvelimen joku muu vastikkeellisen transaktion toteutusyksikön alayksikkö on sovitettu toimittamaan pyydetyt varmennustiedot. Sama tietysti tapahtuu myös kuvioiden 5A ja 5B esimerkissä, vaikkei sitä ole erikseen esitettykään. Esimerkeissä oletetaan, että kassapäätteessä oleva sovellus (laskunhallintayksikkö) ja päätelaitteessa/siirtopalvelimessa oleva sovellus (esimerkiksi vastikkeellisen transaktion toteutusyksikön aliyksikkö) on konfiguroitu laskemaan tiiviste (hash) rahamäärän ja sovelluksen salaisen sarjanumeron summasta, ja tällä tavalla kassapäätteen sovellus voi varmistaa, että päätelaitteen sovellus on muuttumaton (oikea ja aito) ja sitä on juuri käytetty. Lisäksi tässä esimerkissä oletetaan, että viitenumeroon lisätään joku kertakäyttöinen, kassapäätteessä olevan sovelluksen laskun muodostamisen jälkeen generoima numero, ja tästä summasta lasketaan toinen tiiviste (hash). Näin varmistetaan tapahtuman tuoreus. Tulee ymmärtää, että nämä ovat vain esimerkkejä siitä, kuinka varmistaminen voidaan tehdä. Oleellista on, että tieto siitä, kuinka varmistuminen tehdään, on vain näillä luotetuilla sovelluksilla (tai parsereilla).

Kuvion 4 esimerkissä oletetaan, ettei siirtopalvelinta käytetä. Esimerkin soveltaminen siirtopalvelimen sisältävään ratkaisuun on alan ammattilaiselle ilmeistä. Lisäksi kuviossa suojatulla yhteydellä lähetetyt tiedot salataan ennen lähettämistä ja puretaan ennen käyttämistä, mutta selvyyden vuoksi salaamista ja vastaavasti salauksen purkamista ei toisteta tietojen vaihtamisen yhteydessä.

Viitaten kuvioon 4, kassapääte tarjoaa asiakkaalle monta eri maksutapaa, kuten lähimaksamisen. Asiakas kuitenkin valitsee tässä hakemuksessa esitetyn suoramaksusovelluksen. Kassapääte havaitsee kohdassa 4-1 suoramaksusovelluksen valinnan, muodostaa laskun ja koska maksutapana on suoramaksusovellus, laskee kohdassa 4-1 valmiiksi tiivisteen laskun summasta (rahamäärästä) ja

sovelluksen salaisesta sarjanumerosta. Kassapääte myös välittää sähköisesti laskun (viesti 4-2) käyttäjän päätelaitteelle, esimerkiksi NFC-tekniikkaa käyttäen, kuten edellä on kerrottu. Laskun saatuaan päätelaite suorittaa yhdessä verkkopankin kanssa maksamiseen liittyvät toimenpiteet (kohta 4-3, viestit 4-4). Tässä esimerkissä oletetaan, että maksaminen onnistui ja viesti 4-5 ja kohta 4-6 vastaavat kuvion 3B viestiä 3-42 ja kohtaa 3-52. Tässä suoritusmuodossa päätelaite koostettuaan kuitin maksusta lähettää kuitin viestissä 4-7 kassapäätteelle ja ylläpitää muistissaan väliaikaisesti kuittia. Kuitin saatuaan kassapääte on sovitettu varmistamaan, että päätelaitteessa käytettiin oikeaa maksusovellusta ja siksi kassapääte lähettää viestissä 4-8 päätelaitteelle pyynnön laskea tiiviste. Laskettuaan tiivisteen (kohta 4-9) suoramaksusovelluksen salaisen sarjanumeron ja kuitissa olevan rahamäärän summasta päätelaite lähettää tiivisteen viestissä 4-10 kassapäätteelle.

Kassapääte vertaa kohdassa 4-11 viestissä 4-10 saatua tiivistettä kohdassa 4-1 laskemaansa tiivisteeseen. Jos ne ovat samat, on sovellus aito. Tässä esimerkissä oletetaan, että ne ovat samat. (Jos päätelaitteen sovellus ei olisi aito, kassapääte voisi ilmoittaa käyttäjälle esimerkiksi, että maksu epäonnistui.) Koska sovellus varmennettiin aidoksi, kassapääte generoi kohdassa 4-11 kertakäyttöisen luvun x, laskee kohdassa 4-11 kertakäyttöisestä luvusta x ja kohdassa 4-1 muodostetussa laskussa olevasta viitenumerosta tiivisteen sekä lähettää kertakäyttöisen luvun x viestissä 4-12 päätelaitteelle.

Päätelaite laskee kohdassa 4-13 kertakäyttöisen luvun x ja kuitissa olevan viitenumeron summasta tiivisteen ja lähettää sen viestissä 4-14 kassapäätteelle.

Kassapääte vertaa kohdassa 4-15 kohdassa 4-11 laskemaansa tiivistettä viestissä 4-14 vastaanotettuun tiivisteeseen. Jos ne ovat samat, kassapääte luottaa, että lasku on maksettu (transaktio suoritettu, vastine saatu) ja näyttää kohdassa 4-15 maksun suoritetuksi. Jos kohdassa 4-15 havaitaan, että tiivisteet eivät ole samat, näytetään maksu epäonnistuneeksi.

Jos kassapäätteen ja käyttäjän päätelaitteen välille ei muodosteta tiedonsiirtoyhteyttä, voivat sovellukset olla järjestetty näyttämään vastaavat tiedot käyttöliittymässä, jolloin kassapäätteen käyttäjä voi verrata kassapäätteellä näkyvää tiivistettä käyttäjän päätelaitteen näyttämään tiivisteeseen ja molempien käyttäjät voivat syöttää esimerkiksi kassapäätteen käyttäjän valitseman kertakäyttöisen luvun vastaaviin laitteisiinsa (tai kassapäätteen käyttäjä voi kertoa/näyttää kassapäätteen näytölle esitettävän kertakäyttöisen luvun).

20165360 PRH 26-08-2016

Kuvioissa 5A ja 5B esitetään suoritusmuotoa, jossa edellä kuvattu prosessi suoritetaan vain, jos pankista ei saada reaaliajassa varmistusta siitä, että maksu on suoritettu. Kuvioiden 5A ja 5B esimerkissä oletetaan lisäksi, että kassapääte on osa isompaa järjestelmää, joten kuviossa 5A kuvataan kassapäätteen toiminnollisuutta ja kuviossa 5B toiminnollisuutta siinä osassa kassapäätejärjestelmää, joka saa reaaliaikaisesti tietoa tilitapahtumista. Siitä käytetään nimitystä kassajärjestelmä kuvioiden 5A ja 5B selityksen yhteydessä. Lisäksi kuvioissa suojatulla yhteydellä lähetetyt tiedot salataan ennen lähettämistä ja puretaan ennen käyttämistä, mutta selvyyden vuoksi salaamista ja vastaavasti salauksen purkamista ei toisteta tietojen vaihtamisen yhteydessä.

Viitaten kuvioon 5A kassapääte muodostaa vaiheessa 501 laskun, jossa on viitenumero, ja lähettää sen käyttäjän päätelaitteelle vaiheessa 502, kuten edellä on kuvattu. Lisäksi kassapääte lähettää vaiheessa 503 ainakin viitenumeron, mahdollisesti myös muuta tietoa kassajärjestelmään. Sen jälkeen kassapääte odottaa ennalta määritellyn ajan t1, vastaanotetaanko kassajärjestelmältä kuittaus ajassa t1 (vaihe 504). Aika t1 on suhteellisen lyhyt aika, mutta riittävä transaktion suorittamiseen ja tiedon välittämiseen transaktion suorittamisesta (maksun maksamisesta).

Jos ajassa t1 ei saada kassajärjestelmältä kuittausta, että maksu on suoritettu (vaihe 504: ei), laskee kassapääte vaiheessa 505 tiivisteen laskun summasta (rahamäärästä) ja sovelluksen salaisesta sarjanumerosta sovelluksen salaisesta ja varmentaa kohdassa 506 käyttäjän päätelaitteen sovelluksen kuten kuviossa 4 kerrottiin. Tässäkin esimerkissä oletetaan, että sovellus varmennettiin aidoksi. Sen jälkeen kassapääte generoi vaiheessa 507 kertakäyttöluvun ja lähettää sen päätelaitteelle. Samanaikaisesti kassapääte laskee vaiheessa 508 tiivisteen kertakäyttöluvun ja viitenumeron summasta, vastaanottaa päätelaitteelta tiivisteen ja vertailee niitä. Vertailun lopputuloksesta tehty päätelmä (samat tiivisteet- maksu suoritettu, eri tiivisteet-maksu epäonnistui) näytetään vaiheessa 509 kassajärjestelmän käyttäjälle.

Jos ajassa t1 saatiin kassajärjestelmästä kuittaus (vaihe 504:kyllä), näytetään vaiheessa 510 kassajärjestelmän käyttäjälle, että maksu onnistui.

Viitaten kuvioon 5B, kassajärjestelmä saa vaiheessa 511 kassapäätteeltä ainakin viitenumeron ja tarkkailee (vaihe 512), saako siihen ajassa t2 kuittauksen joltain pankkijärjestelmältä. Aika t2 on edullisesti sama tai hiukan lyhyempi kuin kuviossa 5A. Jos kuittaus saadaan ajassa t2 (vaihe 512:kyllä), kassajär-

jestelmä päättelee vaiheessa 513 pankkijärjestelmän kuittauksessa olleen viitenumeron perusteella kassapäätteen, jolle lähettää vaiheessa 514 tiedon maksun suorittamisesta. Jos kuittausta ei saada ajassa t2 (vaihe 512:ei), lopettaa kassajärjestelmä vaiheessa 515 viitenumeron tarkkailun.

Muita vaihtoehtoja varmistaa, että suoramaksusovellusta on juuri käytetty, voidaan luonnollisesti käyttää edellä kuvatun tavan lisäksi tai sen sijaan. Eräs esimerkki on, että tiivisteen laskenta vaihtuu ajan funktiona, edellyttäen että kassapäätteen ja käyttäjän päätelaitteen kellot ovat riittävällä tarkkuudella synkronissa, vaikkapa muutaman sekunnin, mielellään korkeintaan minuutin välein. Eräs toinen esimerkki on, että sovelluspalvelinta pyydetään valitsemaan tiivisteen laskennan rutiini, joka sitten palauttaa joko tiivisteen tai esimerkiksi rutiinin siemenluvun tai vastaavan. jolla tuotetaan tiivistetty varmistus.

Vaikka edellä esitetyissä esimerkeissä puhutaan maksamiseen liittyvästä reaaliaikaisesta vastikkeellista transaktiosta, on alan ammattilaiselle ilmeistä, että edellä esitettyä voidaan soveltaa mihin tahansa reaaliaikaiseen vastikkeelliseen transaktioon. Kuviossa 6 esitetään periaatteellinen, erittäin pelkistetty kaavio vastikkeellisen transaktion tiedon- tai tarvikkeen siirtymisestä transaktiojärjestelyn osapuolien välillä.

Viitaten kuvioon 6 vastikkeen haluaja 1 (transaktiossa tarvittavien tietojen pyytäjä) näyttää tai muulla tavoin osoittaa vastikkeen haltijalle eli vastineen saajalle 2 haluamansa vastikkeen 4. Vastineen saaja 2 puolestaan välittää vastikkeen haluajalle 1 ainakin tiedon vastineesta 5 ja siitä, mihin vastine tulisi suorittaa (tai kohdentaa), eli muut (saajan) tiedot. Tieto vastineesta voi myös osoittaa transaktion tyypin tai tieto tyypistä voidaan tarvittaessa antaa muutenkin. Vastikkeen haluaja 1 välittää ainakin vastineen ja saajan tiedot 6 transaktion suorittajalle 3, joka transaktion suoritettuaan palauttaa vahvistuksen 7 suoritetusta transaktiosta vastikkeen haluajalle 1. Tämä puolestaan näyttää tai muulla tavoin osoittaa vahvistuksen 8 vastineen saajalle 2, joka antaa tai muulla tavoin välittää 9 vastikkeen vastikkeen haluajalle 1. Transaktion suorittaja 3 lähettää tiedon 10 transaktiosta myös vastineen saajalle 2, eli vastineen vastaanottajalle, joka tiedonsiirtoviiveistä ja/tai sovellusmuodosta riippuen voi saada tiedon siitä heti tai jonkun ajan kuluessa. Jos järjestelmä on sellainen, että tieto/vahvistus välittyy reaaliaikaisesti vastineen saajalle, vastikkeen haluajan ei tarvitse näyttää tai osoittaa vahvistusta.

Käytettäessä edellä kuvattuja esimerkkejä vastike on ostos tai ostokset, vastikkeen haluaja 1 on ostajan päätelaite tai ostajan päätelaitteen ja siirtopalvelimen yhdistelmä, transaktio on tietyn rahamäärän siirtyminen ostajalta myyjälle,

vastineen eli rahamäärän saaja 2 on kauppa, vastine 5 on esitetty laskussa, tiedoissa 6 kulkee mm. kaupan ja vastineen (rahamäärän) tiedot pankkijärjestelmään, joka on transaktion suorittaja 3. Se palauttaa vahvistuksena 7 varmennuksen maksusta ja tietona 10 tiedon tilille tulleesta rahamäärästä.

Toisessa esimerkissä vastike on laina, vastikkeen haluaja 1 on lainanottaja, transaktion saaja 2 on pankki tai muu lainaaja, vastine 5 on tieto vakuudesta, tiedoissa 6 kulkee mm. pankin ja vakuuden tiedot lainajärjestelmään, joka on transaktion suorittaja 3. Se palauttaa vahvistuksena 7 varmennuksen vakuudesta ja tietona 10 tiedon asetetusta vakuudesta.

Eräässä toisessa esimerkissä vastike on kirjastosta lainattava materiaali, vastikkeen haluaja 1 on lainaajan päätelaite, transaktion saaja 2 on kirjasto, vastine 5 on materiaalin identifiointitieto, joka kulkee tiedoissa 6. Transaktion suorittaja 3 on kirjastojärjestelmä, joka palauttaa vahvistuksena 7 kuitin lainauksesta ja tietona 10 lainaustiedon.

Edellä kuvioiden 2-6 yhteydessä kuvatut vaiheet/kohdat, sanomat ja liittyvät toiminnot eivät ole absoluuttisessa aikajärjestyksessä ja joitakin vaiheita/kohtia voidaan suorittaa samanaikaisesti tai annetusta järjestyksestä poiketen ja/tai jättää pois. Muita toimintoja voidaan myös suorittaa vaiheiden/kohtien välissä tai vaiheiden/kohtien sisällä ja muita sanomia voidaan lähettää havainnollistettujen sanomien välissä. Esimerkiksi maksun varmistamiseksi ja/tai maksun suorittamiseksi voidaan tarvita useampiakin haastevasteita. Toinen esimerkki on, että käyttäjän päätelaite piippaa, kun maksu on suoritettu onnistuneesti. Eräs esimerkki on se, että käyttäjälle voidaan näyttää kuvioista 7A-7C vain kuvion 7C valinta, tai ei edes sitä. Epäonnistunutta transaktiota tai muuta virhetilannetta voidaan yrittää myös ratkaista automaattisesti, esimerkiksi pyytämällä tietoja uudestaan. Kuvatut toiminnot havainnollistavat kyseessä olevissa laitteissa proseduureja, jotka voidaan toteuttaa yhteen tai useampaan fyysiseen tai loogiseen entiteettiin. Sanomat ovat vain esimerkinomaisia ja ne voivat jopa käsittää useita erillisiä sanomia saman tiedon lähettämiseksi. Sanomat voivat lisäksi sisältää muuta tietoa kuin edellä esitetyt tiedot. Myös muita sanomia voidaan lähettää. Esimerkiksi, jos kassapäätteellä on yhteys siirtopalvelimeen, kassapääte voi lähettää laskun, jonka joko näyttää näytöllään tai välittää käyttäjän päätelaitteelle, myös siirtopalvelimelle. Siirtopalvelin voi olla järjestetty liittämään toisiinsa tämä kassapäätteeltä saatu lasku ja päätelaitteelta saatava transaktiopyyntö toisiinsa esimerkiksi viitenumeron perusteella, ja kun lasku on saatu maksetuksi, lähettämään tiedon maksun onnistumisesta myös kassapäätteelle, jolloin kassapääte saa tiedon suoraan

luotettavalta taholta eikä muita varmistuksia tarvita. Tätä tarkoitusta varten siirtopalvelin voi käsittää kolmannen salausavainkukkaron vastinparin (salausavainkukkaro kassajärjestelmän ja siirtopalvelimen välillä). Myös muunlaisia palvelinratkaisuja voidaan käyttää.

Edellä esitettyjen esimerkkien perusteella on selvää, että reaaliaikainen vastikkeellinen transaktio onnistuu turvallisesti.

Päätelaite tai siirtopalvelin tai kassajärjestelmä tai vastaava(t) laite(laitteet) tai laitteiden yhdistelmä(t), joka toteuttaa yhden tai useamman jonkun edeltävän, kuvioiden 2 -6 yhteydessä kuvatun suoritusmuodon tai erillisen esimerkin yhteydessä kuvatun toiminnollisuuden, käsittää tunnetun tekniikan mukaisten välineiden lisäksi välineitä yhden tai useamman jonkun suoritusmuodon/esimerkin yhteydessä kuvatun päätelaitteen, siirtopalvelimen tai jonkun niiden yhteydessä kuvatun yksikön toiminnollisuuden toteuttamiseksi, ja se voi käsittää erilliset välineet kullekin erilliselle toiminnolle tai välineet voidaan konfiguroida toteuttamaan kaksi tai useampi toiminto. Päätelaite ja/tai siirtopalvelin voidaan konfiguroida tietokoneena tai mikroprosessorina, kuten yhdelle mikropiirille integroituna elementtinä, joka sisältää ainakin muistia aritmeettisen operaation käyttämän tallennusalueen aikaansaamiseksi ja toimintaprosessorin aritmeettisen operaation suorittamiseksi.

Kuvio 8 on yksinkertaistettu lohkokaavio, joka havainnollistaa joitakin yksiköitä, joita laite 800, joka on konfiguroitu olemaan käyttäjän päätelaite, tai ainakin käsittämään tallennusyksikön ja/tai vastikkeellisen transaktion toteutusyksikön tai jonkun sen aliyksikön tai vastaavan yksikön, joka on sovitettu suorittamaan vastaavat, kuvioiden 2-4 yhteydessä kuvatut toiminnollisuudet tai osan toiminnollisuuksista. Kuvion 8 esimerkissä laite 800 käsittää yhden tai useamman liitynnän (IFs) 801 ollakseen tiedonsiirtoyhteydessä muiden laitteiden, kuten transaktion suoritusjärjestelmän laitteiden ja/tai transaktion kohdejärjestelmän laitteiden, kanssa, yhden tai useamman suorittimen (PROC.) 802, joka on konfiguroitu suorittamaan vastikkeellisen transaktion toteutusyksikön ja/tai tallennus- ja/tai transaktion tiedonsiirtoyksikön tai ainakin sen jonkun aliyksikön toiminnollisuutta vastaavan algoritmin/vastaavien algoritmien (ALG.) 803 kanssa, ja muistia (MEM) 804 käytettäväksi tallentamaan ainakin algoritmin/algoritmit tai vastaavan toimintaohjejoukon sekä aikaansaamaan suojattu muisti sinne tallennettaville tiedoille, sekä lisäksi yhden tai useamman käyttäjän rajapinnan (U-IF) 801' vuorovaikutukseen käyttäjän kanssa.

20165360 PRH 26-08-2016

Kuvio 9 on yksinkertaistettu lohkokaavio, joka havainnollistaa joitakin yksiköitä, joita laite 900, joka on konfiguroitu olemaan siirtopalvelin, tai ainakin käsittämään vastikkeellisen transaktion tietojensiirtoyksikön tai jonkun sen aliyksikön tai vastaavan yksikön, joka on sovitettu suorittamaan vastaavat, kuvioiden 2-4 yhteydessä kuvatut toiminnollisuudet tai osan toiminnollisuuksista. Kuvion 9 esimerkissä laite 900 käsittää yhden tai useamman liitynnän (IFs) 901 ollakseen tiedonsiirtoyhteydessä muiden laitteiden, kuten transaktion suoritusjärjestelmän laitteiden ja/tai transaktion kohdejärjestelmän laitteiden, kanssa, yhden tai useamman suorittimen (PROC.) 902, joka on konfiguroitu suorittamaan vastikkeellisen transaktion tietojensiirtoyksikön tai ainakin sen jonkun aliyksikön toiminnollisuutta vastaavan algoritmin/vastaavien algoritmien (ALG.) 903 kanssa, ja muistia (MEM) 904 käytettäväksi tallentamaan ainakin algoritmin/algoritmit tai vastaavan toimintaohjejoukon. Tulee ymmärtää, että siirtopalvelin voidaan toteuttaa myös hajautettuna palvelimena tai pilvipalvelimena.

Kuvio 10 on yksinkertaistettu lohkokaavio, joka havainnollistaa joitakin yksiköitä, joita vastineen vastaanottajan (saajan) laitteisto 1000, joka on konfiguroitu käsittämään laskunhallintayksikön tai jonkun sen aliyksikön tai vastaavan yksikön, joka on sovitettu suorittamaan joko yhdessä tai useamman laitteen/laskunhallintayksikön yhdistelmänä kuvioiden 4, 5A ja 5B yhteydessä kuvatut toiminnollisuudet tai osan toiminnollisuuksista. Kuvion 10 esimerkissä laite 1000 käsittää yhden tai useamman liitynnän (IFs) 1001 ollakseen tiedonsiirtoyhteydessä muiden laitteiden, kuten käyttäjän päätelaitteen ja laitteiston muoden laitteiden kanssa, yhden tai useamman suorittimen (PROC.) 1002, joka on konfiguroitu suorittamaan laskunhallintayksikön tai ainakin sen jonkun aliyksikön toiminnollisuutta vastaavan algoritmin/vastaavien algoritmien (ALG.) 1003 kanssa, ja muistia (MEM) 1004 käytettäväksi tallentamaan ainakin algorit-min/algoritmit tai vastaavan toimintaohjejoukon. Muistista osa voi olla suojattua muistia. Tulee ymmärtää, että laitteisto voidaan toteuttaa myös hajautettuna ja/tai pilvipalvelinta hyödyntäen.

Suoritin 802, 902, 1002 voi esimerkiksi olla keskusyksikkö, toimintaprosessori, logiikkapiiri, sovelluskohtainen mikropiiri (ASIC, application-specific integrated circuits), ja uudelleenohjelmoitava digitaalinen logiikkapiiri FPGA (field-programmable gate array).

Muisti 804, 904, 1004 voi olla keskitetty tai hajautettu muisti ja se voidaan toteuttaa millä tahansa muistiteknologialla tai niiden yhdistelmänä, kuten puolijohdemuistina, flash-muistina, magneettimuistina, ja optisena muistina.

Muisti tai sen osa voi olla myös kiinteä osa laitetta 800, 900, laitteistoa 1000 tai laitteiden yhdistelmää tai irrotettava muisti tai laitteen ulkopuolinen muisti.

Eräässä suoritusmuodossa aikaansaadaan tietokoneohjelma, joka on sisällytetty mille tahansa suorittimella tai tietokoneella luettavalle datan tallennusvälineelle, ja joka käsittää ohjelmaohjeita, jotka, kun ne on ladattu suorittimen sisältävään laitteeseen, ovat osa vastikkeellista transaktion toteutusyksikköä ja/tai tallennusyksikköä ja/tai vastikkeellisen transaktion tietojensiirtoyksikköä ja/tai laajennettua vastikkeellista transaktion toteutusyksikköä ja/tai laskunhallintayksikköä.

Tulee ymmärtää, että myös muita yksiköitä voidaan toteuttaa erilaisilla piireillä/suorittimilla, mikro-ohjelmistona/mikro-ohjelmistoina ja/tai ohjelmistona/ohjelmistoina.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä reaaliaikaisen vastikkeellisen transaktion toteuttamiseksi, joka menetelmä käsittää:

ylläpidetään muistissa yhtä tai useampaa reaaliaikaista transaktion suoritusjärjestelmää varten vastaavasti yhtä tai useampaa parseria reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten transaktioon liittyvien pyyntöjen luomiseksi ja vastausten sisällön tunnistamiseksi;

ylläpidetään suojatussa muistissa transaktion suorittamiseen tarvittavia, pyytäjäkohtaisia tietoja salattuna;

vastaanotetaan (202, 3-3, 5) reaaliaikaisen transaktion suorittamiseksi vastikkeesta vaadittava vastine ja vastineen saajan tietoja;

varmennetaan (201, 3-1, 3-2) transaktion pyytäjän oikeus käyttää transaktion suorittamiseen tarvittavia salattuja pyytäjäkohtaisia tietoja;

jos transaktion pyytäjällä on oikeus käyttää suorittamiseen tarvittavia salattuja pyytäjäkohtaisia tietoja, menetelmä käsittää lisäksi:

puretaan suojatussa muistissa salaus ainakin osasta pyytäjäkohtaisia transaktion suorittamiseen tarvittavia tietoja;

muodostetaan (3-5, 3-6) suojattu yhteys transaktion reaaliaikaiseen suoritusjärjestelmään;

muodostetaan (3-29) parseria käyttäen reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukainen transaktiopyyntö, joka sisältää vastineen, saajan tietoja ja ainakin yhden transaktion suorittamiseen tarvittavan pyytäjäkohtaisen tiedon salaamattomana;

lähetetään (3-30, 6) transaktiopyyntö suojatulla yhteydellä reaaliaikaiseen transaktion suoritusjärjestelmään; ja

vastaanotetaan (3-43, 3-42, 7, 10) reaaliaikaiselta transaktion suoritusjärjestelmältä suojatulla yhteydellä transaktiovastaus, joka osoittaa, suoritettiinko transaktiopyyntö onnistuneesti.

2. Patenttivaatimuksen 1 mukainen menetelmä, joka lisäksi käsittää, jos transaktion pyytäjällä on oikeus käyttää suorittamiseen tarvittavia salattuja pyytäjäkohtaisia tietoja:

vastaanotetaan (3-34) reaaliaikaiselta transaktion suoritusjärjestelmältä suojatulla yhteydellä lisätietopyyntö, joka käsittää yhden tai useamman tietyn tiedon pyynnön reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisesti;

tunnistetaan (3-35) parseria käyttäen pyydetyt yksi tai useampi tietty tieto;

haetaan transaktion suorittamiseen tarvittavista salauksesta puretuista pyytäjäkohtaisista tiedoista pyydetyt yksi tai useampi tietty tieto;

muodostetaan (3-39) parseria käyttäen reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukainen vastaus, joka sisältää pyydetyt yhden tai useamman tietyn tiedon salaamattomana;

lähetetään (3-40) vastaus suojatulla yhteydellä reaaliaikaiselle suoritusjärjestelmälle.

3. Patenttivaatimuksen 2 mukainen menetelmä, joka lisäksi käsittää pyydetyn yhden tai useamman pyytäjäkohtaisen tiedon salauksen purkamisen, jos ne ovat vielä salattuja.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, joka lisäksi käsittää:

ylläpidetään kahta tai useampaa reaaliaikaista suoritusjärjestelmää varten kullekin suoritusjärjestelmälle parseria reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten transaktioon liittyvien pyyntöjen luomiseksi ja vastausten sisällön tunnistamiseksi;

valitaan (3-4) transaktion reaaliaikainen suoritusjärjestelmä kahden tai useamman reaaliaikaisen transaktion suoritusjärjestelmän joukosta; ja

käytetään valitun reaaliaikaisen transaktion suorittajan parseria.

5. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, joka lisäksi käsittää:

pyydetään (209) käyttöliittymän välityksellä transaktion pyytäjältä vahvistus transaktiolle; ja

lähetetään transaktiopyyntö vain, jos käyttöliittymän kautta saadaan vahvistus.

6. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, joka lisäksi käsittää, jos transaktio voidaan suorittaa useammasta eri lähteestä:

pyydetään (206) käyttöliittymän välityksellä transaktion pyytäjää valitsemaan lähde; ja

muodostetaan suojattu yhteys siihen transaktion reaaliaikaiseen suoritusjärjestelmään, jossa valittu lähde on.

7. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, joka lisäksi käsittää:

jos transaktiopyyntö suoritettiin onnistuneesti, lähetetään (3-48, 10) tieto transaktion onnistumisesta myös laitteelle, jolta vastaanotettiin vastikkeesta vaadittava vastine ja saajan tietoja.

8. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, joka lisäksi käsittää:

jos transaktiopyyntö suoritettiin onnistuneesti, lähetetään (3-42) tieto transaktion onnistumisesta myös saajan tietojen osoittamaan paikkaan.

9. Tietokoneohjelmistotuote, joka tietokoneella ajettuna aikaansaa tietokoneen suorittamaan jonkin edellisen patenttivaatimuksen 1-7 mukaisen menetelmän.

10. Laite (120,120a, 140), joka käsittää ainakin

tiedonsiirtovälineet (123, 143) transaktion suoritusjärjestelmän kanssa kommunikoimiseksi;

t u n n e t t u siitä, että laite käsittää lisäksi:

muistia (122, 142), jonne on tallennettu ainakin yksi parseri reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten transaktioon liittyvien pyyntöjen luomiseksi ja vastausten sisällön tunnistamiseksi, ja josta muistista ainakin osa on suojattua muistia (122-3), jonne on tallennettu transaktiossa tarvittavaa pyytäjäkohtaista tietoa; ja

transaktiovälineet (122-1, 122-1a, 141) jonkin patenttivaatimuksen 1-7 mukaisen menetelmän suorittamiseksi.

11. Patenttivaatimuksen 10 mukainen laite (120,120a, 140), joka on konfiguroitu varmentamaan transaktiovälineet ennen jonkin patenttivaatimuksen 1-7 mukaisen menetelmän suorittamiseksi.

12. Patenttivaatimuksen 10 tai 11 mukainen laite (120,120a, 140), joka on konfiguroitu varmentamaan, että jonkin patenttivaatimuksen 1-7 mukainen menetelmä on suoritettu oikealla sovelluksella ja tietyn ajan sisällä.

13. Patenttivaatimuksen 10, 11 tai 12 mukainen laite (120,120a), joka on käyttäjän päätelaite, joka lisäksi käsittää käyttöliittymän tietojen välittämiseksi käyttäjälle ja käyttäjän syötteiden vastaanottamiseksi.

14. Patenttivaatimuksen 10, 11 tai 12 mukainen laite (140), joka on siirtopalvelin, jossa tiedonsiirtovälineet on sovitettu kommunikoimaan käyttäjien päätelaitteiden kanssa suojatun yhteyden yli.

15. Laite (140), joka käsittää ainakin

tiedonsiirtovälineet (143) käyttäjän päätelaitteen (120) ja reaaliaikaisen transaktion suoritusjärjestelmän kanssa kommunikoimiseksi;

t u n n e t t u siitä, että:

laite käsittää lisäksi parserin (142-2) kutakin reaaliaikaista transaktion suoritusjärjestelmää varten reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten transaktioon liittyvien pyyntöjen luomiseksi ja vastausten sisällön tunnistamiseksi;

laitteen (140) ollessa sovitettu vastaanotettuaan käyttäjän päätelaitteelta vastikkeesta vaadittavan vastineen, vastineen saajan tietoja ja tiedon valitusta reaaliaikaisesta transaktion suoritusjärjestelmästä, jota päätelaitteen käyttäjä haluaa käyttää vastineen suorittamiseksi saajalle, valitsemaan valitun transaktion suoritusjärjestelmän perusteella parseri, muodostamaan suojattu yhteys transaktion reaaliaikaiseen suoritusjärjestelmään (130), hakemaan ainakin yhden transaktion suorittamiseen tarvittavan pyytäjäkohtaisen tiedon, jota säilytetään salattuna, muodostamaan reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisen transaktiopyynnön, joka sisältää vastineen, saajan tietoja ja ainakin yhden transaktion suorittamiseen tarvittavan pyytäjäkohtaisen tiedon salaamattomana, lähettämään transaktiopyyntö transaktion reaaliaikaiseen suoritusjärjestelmään (130) ja vastaanottamaan transaktiovastaus, joka osoittaa, suoritettiinko transaktiopyyntö onnistuneesti.

16. Järjestelmä (100), joka käsittää

ainakin yhden käyttäjän päätelaitteen (120);

ainakin yhden siirtopalvelimen (140); ja

ainakin yhden transaktion reaaliaikaisen suoritusjärjestelmän (130);

välineitä (122-2) ylläpitämään transaktion suorittamiseen tarvittavia pyytäjäkohtaisia tietoja salattuna joko käyttäjän päätelaitteessa tai siirtopalvelimessa ja purkamaan tilapäisesti salaus ainakin osasta transaktion suorittamiseen tarvittavia pyytäjäkohtaisia tietoja;

jossa järjestelmässä (100)

käyttäjän päätelaite (120) sisältää suojatussa muistissa (122) sovelluksen (122-1) reaaliaikaista transaktiota varten ja ainakin tietoa (122-3), jolla käyttäjän oikeus käyttää sovellusta voidaan varmentaa, käyttäjän päätelaitteen ollessa sovitettu välittämään käyttäjän varmennuksen onnistumisen jälkeen ainakin vastikkeesta vaadittavan vastineen ja vastineen saajan tietoja siirtopalvelimelle,

t u n n e t t u siitä, että

siirtopalvelin (140) on sovitettu olemaan yhteydessä käyttäjän päätelaitteeseen (120) ja reaaliaikaiseen transaktion suoritusjärjestelmään (130) ja käsittää reaaliaikaista transaktion suoritusjärjestelmää varten parserin (142-2) reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten transaktioon liittyvien pyyntöjen luomiseksi ja vastausten sisällön tunnistamiseksi, siirtopalvelimen (140) ollessa sovitettu vastaanotettuaan käyttäjän päätelaitteelta vastikkeesta vaadittavan vastineen ja vastineen saajan tietoja muodostamaan suojattu yhteys transaktion reaaliaikaiseen suoritusjärjestelmään (130), hakemaan ainakin yhden transaktion suorittamiseen tarvittavan pyytäjäkohtaisen tiedon, muodostamaan reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisen transaktiopyynnön, joka sisältää vastineen, vastineen saajan tietoja ja ainakin yhden transaktion suorittamiseen tarvittavan pyytäjäkohtaisen tiedon salaamattomana, lähettämään transaktiopyyntö transaktion reaaliaikaiseen suoritusjärjestelmään (130) ja vastaanottamaan transaktiovastaus, joka osoittaa, suoritettiinko transaktiopyyntö onnistuneesti.

17. Patenttivaatimuksen 16 mukainen järjestelmä (100), jossa

siirtopalvelin (140) on sovitettu vastaanottamaan transaktion reaaliaikaiselta suoritusjärjestelmältä (130) yhden tai useamman pyytäjäkohtaisen tunnuspyynnön, hakemaan pyytäjäkohtaisista tiedoista pyydetyn tunnuksen tai tunnukset ja lähettämään ne transaktion reaaliaikaiseen suoritusjärjestelmään (130).

18. Patenttivaatimuksen 16 tai 17 mukainen järjestelmä (100), joka käsittää ainakin kaksi eri transaktion reaaliaikaista suoritusjärjestelmää (130); ja

käyttäjän päätelaite on konfiguroitu välittämään vastikkeesta vaadittavan vastineen ja vastineen saajan tietojen lisäksi tiedon valitusta reaaliaikaisesta transaktion suoritusjärjestelmästä, jota päätelaitteen käyttäjä haluaa käyttää vastineen suorittamiseksi saajalle, ja

siirtopalvelin (140) käsittää ainakin kutakin reaaliaikaista transaktion suoritusjärjestelmää varten parserin (142-2) reaaliaikaisen transaktion suoritusjärjestelmän asetusten mukaisten pyyntöjen ja vastausten luomiseksi, siirtopalvelimen ollessa sovitettu valitsemaan parserin valitun reaaliaikaisen transaktion suoritusjärjestelmän perusteella.

19. Patenttivaatimuksen 16, 17 tai 18 mukainen järjestelmä (100), jossa transaktion reaaliaikainen suoritusjärjestelmä (130) on verkkopankkijärjestelmä.

Patentkrav

1. Förfarande för att utföra en transaktion mot vederlag i realtid, vilket förfarande innefattar:

att i minnet för ett eller flera system upprätthålla för utförande av en transaktion i realtid respektive en eller flera parsrar för att generera transaktionsbegäran enligt inställningarna i ett system för utförande av en transaktion i realtid och för att identifiera innehållet i svaren;

att i ett skyddat minne i krypterad form upprätthålla begär specifik data som behövs för utförande av transaktionen;

att ta emot (202, 3-3, 5) för att utföra en transaktion i realtid en ersättning som krävs för vederlag och data av mottagaren av ersättningen;

att verifiera (201, 3-1, 3-2) att den som begär transaktionen har rätt att använda krypterad begär specifik data som behövs för utförande av transaktionen;

ifall den som begär transaktionen har rätt att använda krypterade begär specifik data som behövs för utförande, innefattar förfarandet dessutom:

att i det skyddade minnet dekryptera åtminstone en del av begär specifik data som behövs för utförande av transaktionen;

att bilda (3-5, 3-6) en skyddad förbindelse till systemet för utförande av en transaktion i realtid;

att med hjälp av parsern generera (3-29) en transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid, vilken begäran innehåller en ersättning, mottagarens data och i okrypterad form åtminstone en begär specifik data som behövs för utförande av åtminstone en transaktion;

att sända (3-30, 6) transaktionsbegäran med en skyddad förbindelse till systemet för utförande av en transaktion i realtid; och

att ta emot (3-43, 3-42, 7, 10) med en skyddad förbindelse från systemet för utförande av en transaktion i realtid ett transaktionssvar som anger huruvida transaktionsbegäran utfördes med framgång.

2. Förfarande enligt patentkrav 1, som dessutom innefattar, ifall den som begär transaktion har rätt att använda krypterade begär specifik data som behövs för utförande:

att ta emot (3-34) med en skyddad förbindelse från systemet för utförande av en transaktion i realtid en begäran om tilläggsinformation, som innefattar begäran om en eller flera vissa data enligt inställningarna i systemet för utförande av en transaktion i realtid;

att identifiera (3-35) parsern med hjälp av de begärda en eller flera vissa data;

att bland okrypterade begär specifik data som behövs för utförande av transaktionen hämta de begärda en eller flera begärda data;

att med hjälp av parsern generera (3-39) ett svar enligt inställningarna i systemet för utförande av en transaktion i realtid som innehåller de begärda en eller flera begärda data i okrypterad form;

att sända (3-40) svaret med en skyddad förbindelse till systemet för utförande i realtid.

3. Förfarande enligt patentkrav 2, som dessutom innefattar dekryptering av de begärda en eller flera begärda begär specifik data ifall de fortfarande är krypterade.

4. Förfarande enligt något av föregående patentkrav, som dessutom innefattar:

att upprätthålla för två eller flera system för utförande i realtid för respektive utförandesystem en parser för att generera transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid och för att identifiera innehållet i svaren;

att välja (3-4) ett system för utförande av en transaktion i realtid bland ett eller flera system för utförande av en transaktion i realtid; och

att använda parsern för det valda systemet för utförande av en transaktion i realtid.

5. Förfarande enligt något av föregående patentkrav, som dessutom innefattar:

att begära (209) via användargränssnittet en bekräftelse av transaktionen av den som begär transaktionen; och

att sända en transaktionsbegäran endast ifall en bekräftelse erhålls via användargränssnittet.

6. Förfarande enligt något av föregående patentkrav, som dessutom innefattar, ifall transaktionen kan utföras från flera olika källor:

att begära (206) via användargränssnittet att den som begär transaktionen väljer källan; och

att bilda en skyddad förbindelse till det system för utförande av en transaktion i realtid där den valda källan finns.

7. Förfarande enligt något av föregående patentkrav, som dessutom innefattar:

ifall transaktionsbegäran utfördes med framgång, att sända (3-48, 10) information om den genomförda transaktionen även till den anordning, från vilken en ersättning som krävs för vederlag och mottagarens data mottagits.

8. Förfarande enligt något av föregående patentkrav, som dessutom innefattar:

ifall transaktionsbegäran utfördes med framgång, att sända (3-42) information om den genomförda transaktionen även till en plats som mottagarens data anger.

9. Dataprogramprodukt, som vid datorkörning får datorn att utföra ett förfarande enligt något av föregående patentkrav 1-7.

10. Anordning (120,120a, 140), som innefattar åtminstone

dataöverföringsorgan (123, 143) för att kommunicera med systemet för utförande av en transaktion i realtid;

k ä n n e t e c k n a d av att anordningen dessutom innefattar:

ett minne (122, 142), i vilket lagrats åtminstone en parser för att generera transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid och för att identifiera innehållet i svaren, och av vilket minne åtminstone en del är skyddat minne (122-3), i vilket lagrats begär specifik data som behövs vid transaktionen; och

transaktionsorgan (122-1, 122-1a, 141) för att utföra förfarandet enligt något av patentkraven 1-7.

11. Anordning (120,120a, 140) enligt patentkrav 10, som konfigurerats för att verifiera transaktionsorganen innan förfarandet enligt något av patentkraven 1-7 utförs.

12. Anordning (120,120a, 140) enligt patentkrav 10 eller 11, som konfigurerats att verifiera att ett förfarande enligt något av patentkraven 1-7 utförts med det korrekta programmet och inom en viss tid.

13. Anordning (120,120a) enligt patentkrav 10, 11 eller 12, som är användarens terminal som dessutom innefattar ett användargränssnitt för att överföra data till användaren och för att ta emot användarens indata.

14. Anordning (140) enligt patentkrav 10, 11 eller 12 som är en överföringsserver, i vilken dataöverföringsorganen anpassats att kommunicera med användarnas terminaler över en skyddad förbindelse.

15. Anordning (140), som innefattar åtminstone

dataöverföringsorgan (143) för att kommunicera med användarens terminal (120) och systemet för utförande av en transaktion i realtid;

k ä n n e t e c k n a d av att:

anordningen dessutom innefattar en parser (142-2) för respektive system för utförande av en transaktion i realtid för att generera transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid och för att identifiera innehållet i svaren;

varvid anordningen (140) anpassats att, efter det den från användarens terminal mottagit en ersättning som krävs för vederlaget data av mottagaren av ersättningen och data av ett valt system för utförande av en transaktion i realtid som användare av terminalen vill använda för utförande av ersättningen till mottagaren, på basis av valda systemet för utförande av en transaktion välja en parser, att bilda en skyddad förbindelse till systemet (130) för utförande av en transaktion i realtid, att hämta begär specifik data som lagras i krypterad form och som behövs för att utföra åtminstone en transaktion, att generera en transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid, som innehåller en ersättning, mottagarens data och åtminstone en okrypterade begär specifik data av data som behövs för utförande av en transaktion, att sända en transaktionsbegäran till systemet (130) för utförande av en transaktion i realtid och att ta emot ett transaktionssvar, som anger huruvida transaktionsbegäran utfördes med framgång.

16. System (100), som innefattar

åtminstone en användarterminal (120);

åtminstone en överföringsserver (140); och

åtminstone ett system (130) för utförande av en transaktion i realtid;

organ (122-2) för att upprätthålla krypterade begär specifik data som behövs för utförande av transaktionen antingen i användarens terminal eller i överföringsservern och för att tillfälligt dekryptera åtminstone en del av begär specifik data som behövs för utförande av transaktionen;

i vilket system (100)

användarens terminal (120) i ett skyddat minne (122) innehåller ett program (122-1) för transaktionen i realtid och åtminstone data (122-3), med vilka användarens rättighet att använda programmet kan verifieras, varvid användarens terminal anpassats att efter genomförd verifiering av användaren förmedla åtminstone en ersättning som krävs för vederlaget och data av en mottagar av ersättningen till överföringsservern,

k ä n n e t e c k n a t av att

överföringsservern (140) anpassats att vara i förbindelse till användarens terminal (120) och till systemet (130) för utförande av en transaktion i realtid och innefattar för systemet för utförande av en transaktion i realtid en parser (142-2) för att generera transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid och för att identifiera innehållet i svaren, varvid överföringsservern (140) anpassats att, sedan den från användarens terminal tagit emot en ersättning som krävs för vederlaget och data av mottagaren av ersättningen, bilda en skyddad förbindelse till systemet (130) för utförande av en transaktion i realtid, hämta begär specifik data som behövs för utförande av åtminstone en transaktion, generera en transaktionsbegäran enligt inställningarna i systemet för utförande av en transaktion i realtid, som innehåller en ersättning, data av mottagaren av ersättningen och åtminstone en okrypterade begär specifik data av data som behövs för utförande av en transaktion, sända en transaktionsbegäran till systemet (130) för utförande av en transaktion i realtid och ta emot ett transaktionssvar, som anger huruvida transaktionsbegäran utfördes med framgång.

17. System (100) enligt patentkrav 16, varvid

överföringsservern (140) anpassats att från systemet (130) för utförande av en transaktion i realtid ta emot en eller flera begär specifika

20165360 PRH 16-08-2018

kodbegäran, att hämta från den begär specifika data den begärda koden eller koderna och att sända dem till systemet (130) för utförande av en transaktion i realtid.

18. System (100) enligt patentkrav 16 eller 17, innefattande åtminstone två system (130) för utförande av en transaktion i realtid;

användarens terminal konfigurerats för att förmedla, utöver ersättningen som krävs för vederlaget och data av mottagaren av ersättningen, data av det valda systemet för utförande av en transaktion i realtid som användare av terminal vill använda för utförande av ersättningen till mottagaren, och

överföringsservern (140) innefattar åtminstone för respektive system för utförande av en transaktion i realtid en parser (142-2) för att generera begäran och svar enligt inställningarna i systemet för utförande av en transaktion i realtid, varvid överföringsservern anpassats att välja en parser på basis av mottagarens data.

19. System (100) enligt patentkrav 16, 17 eller 18, i vilket systemet (130) för utförande av en transaktion i realtid är ett nätbankssystem.

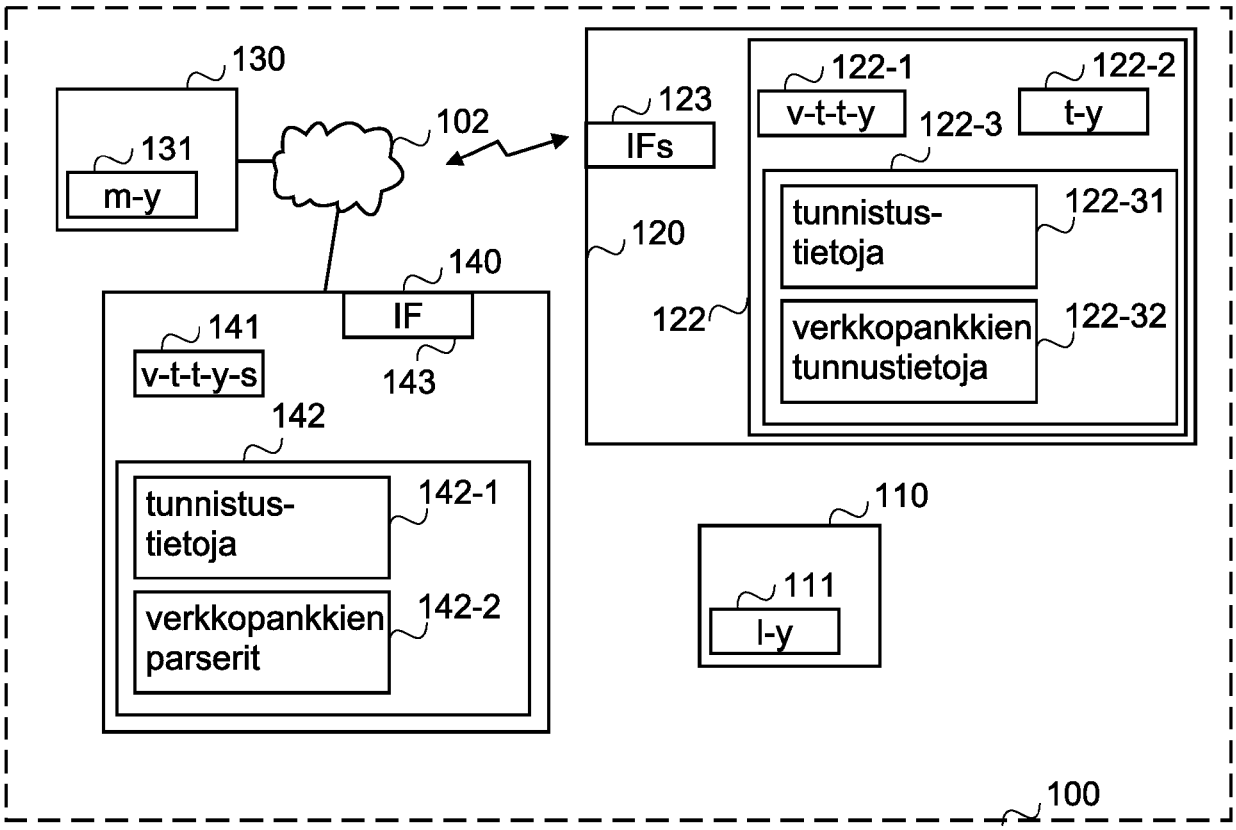


FIG.1A

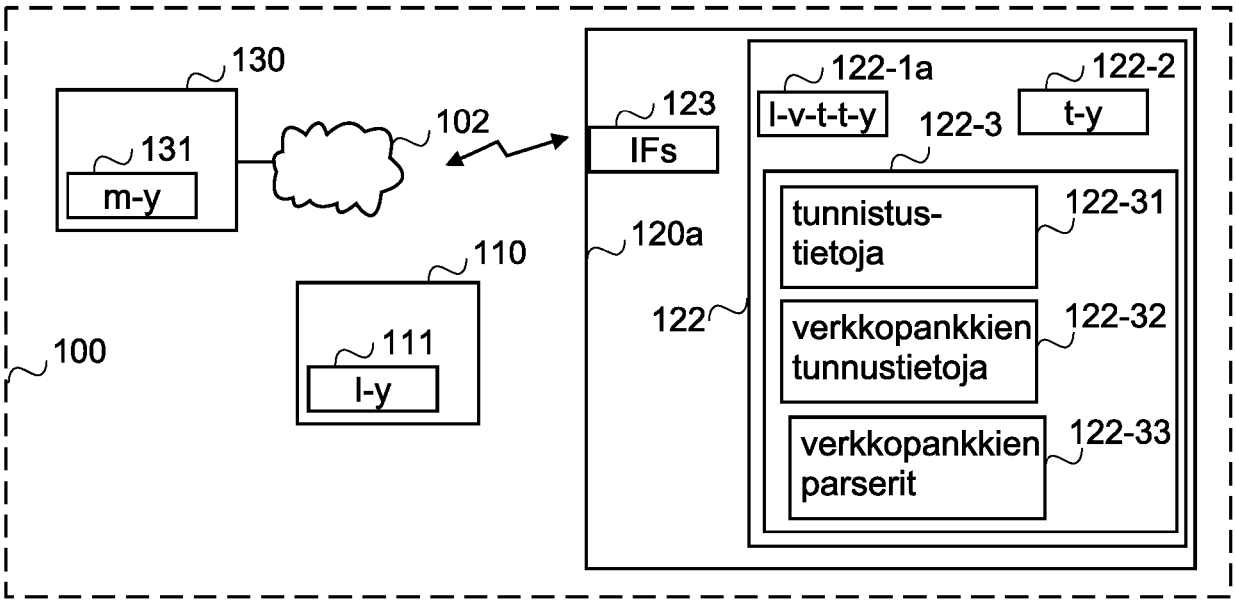


FIG.1B

20165360 PRH 25-08-2016

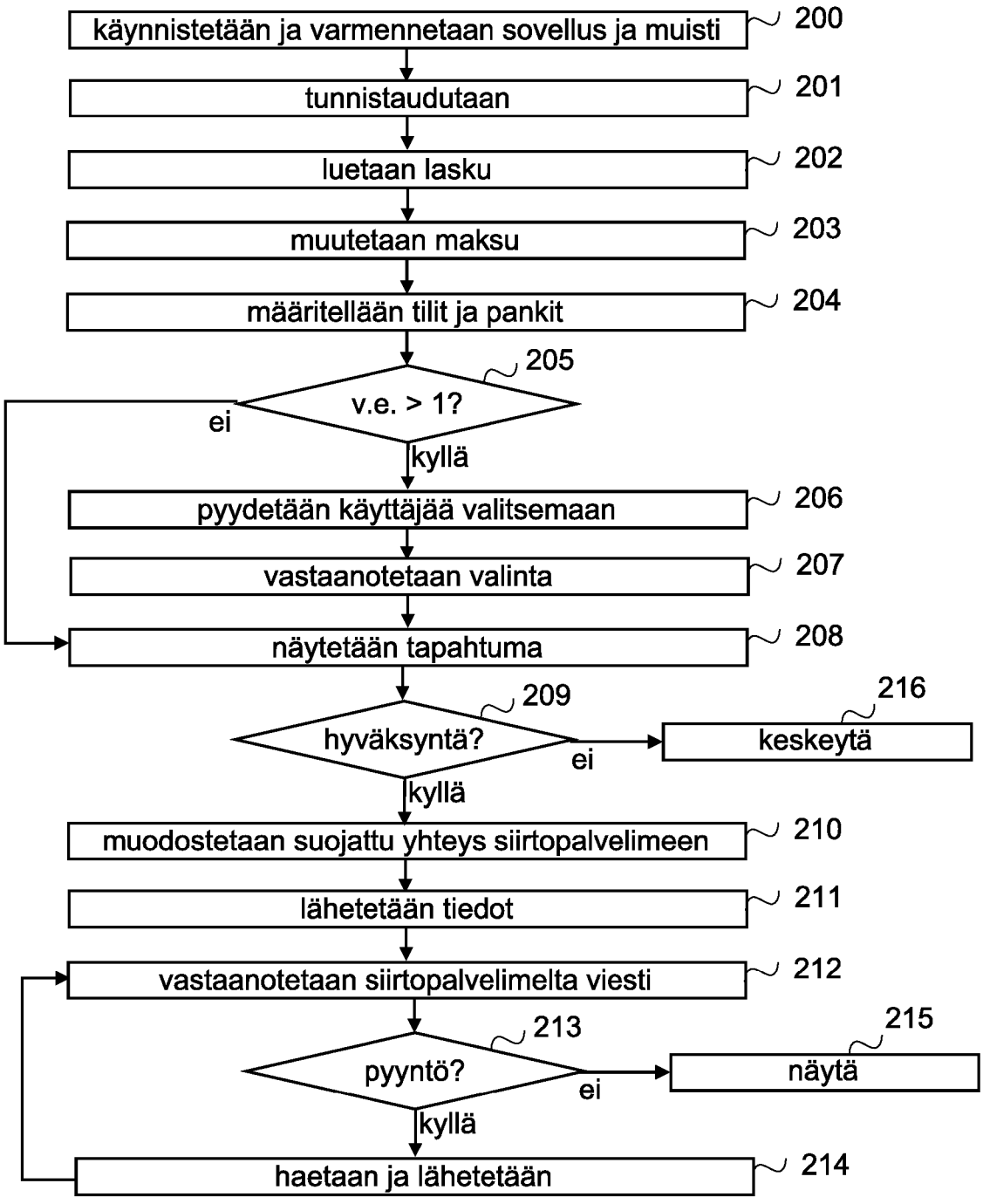


FIG.2

20165360 PRH 25-08-2016

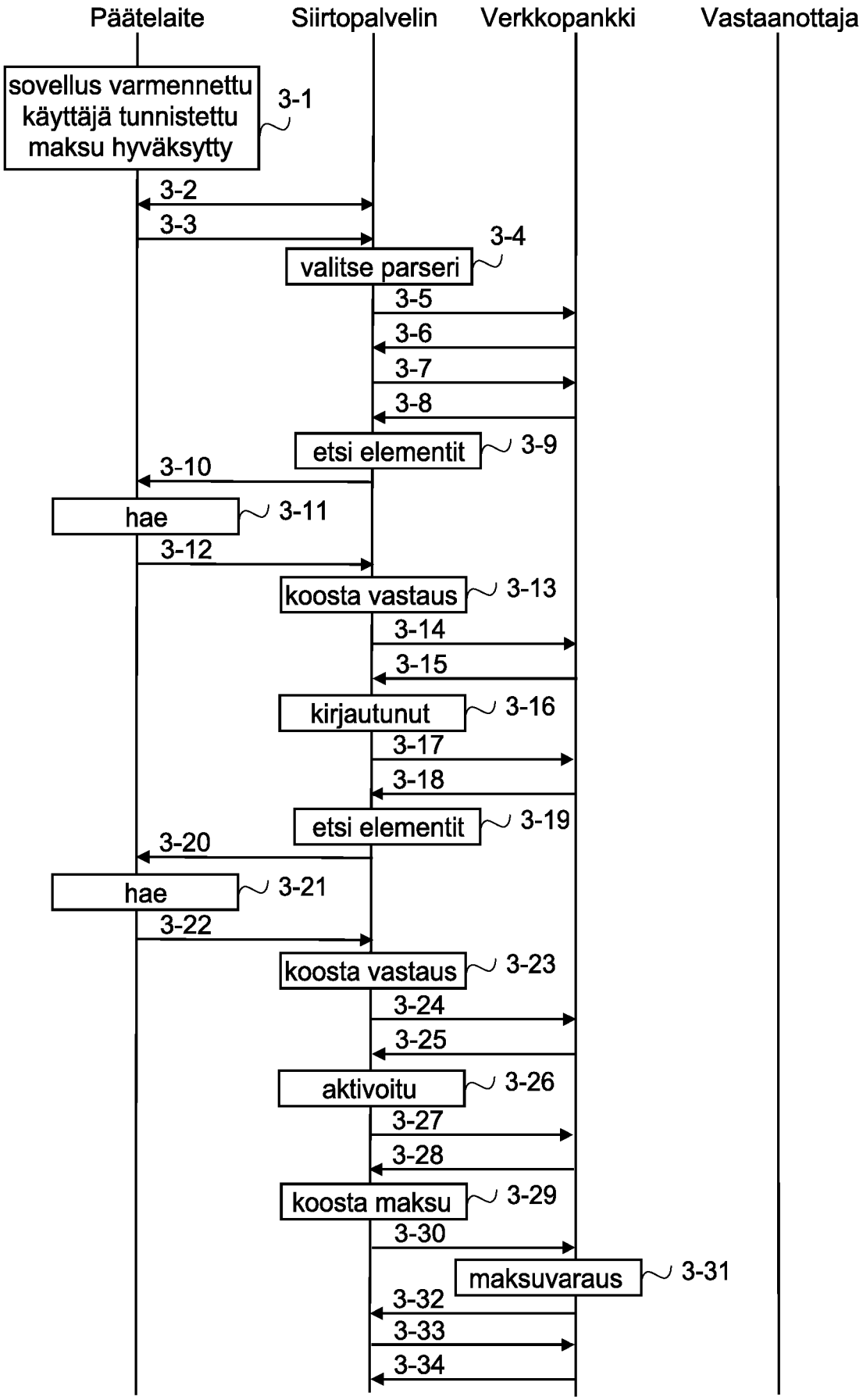


FIG.3A

20165360 PRH 25-08-2016

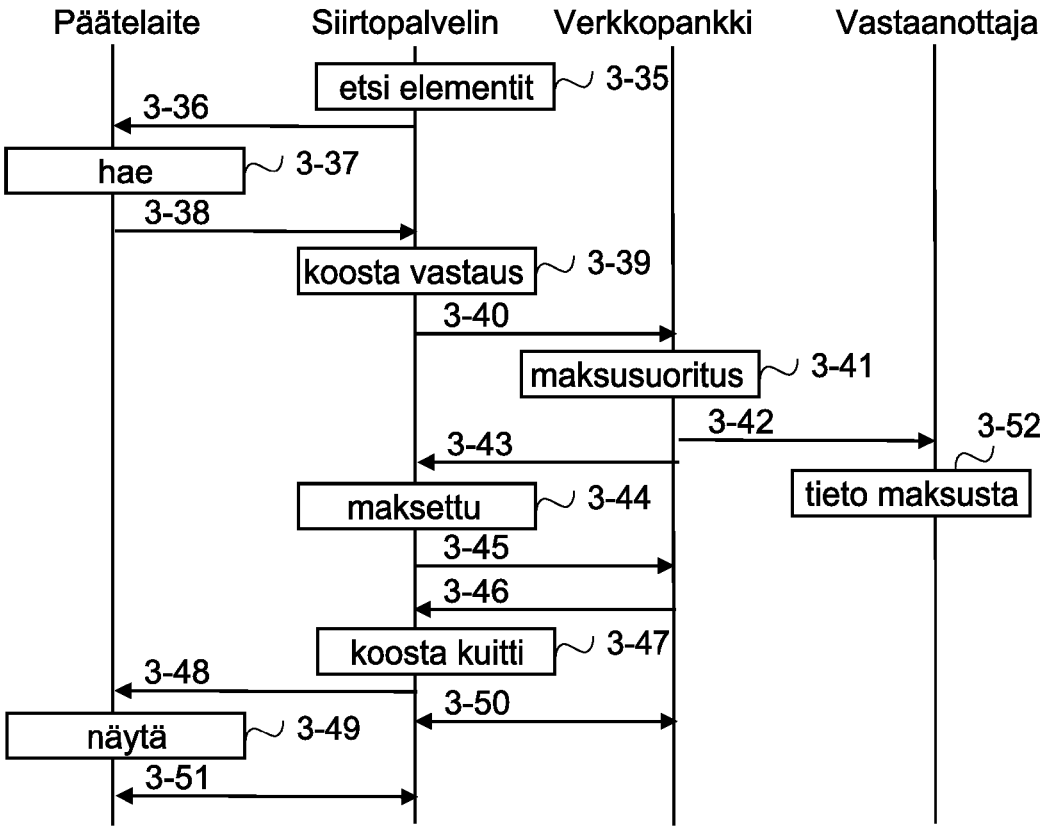


FIG.3B

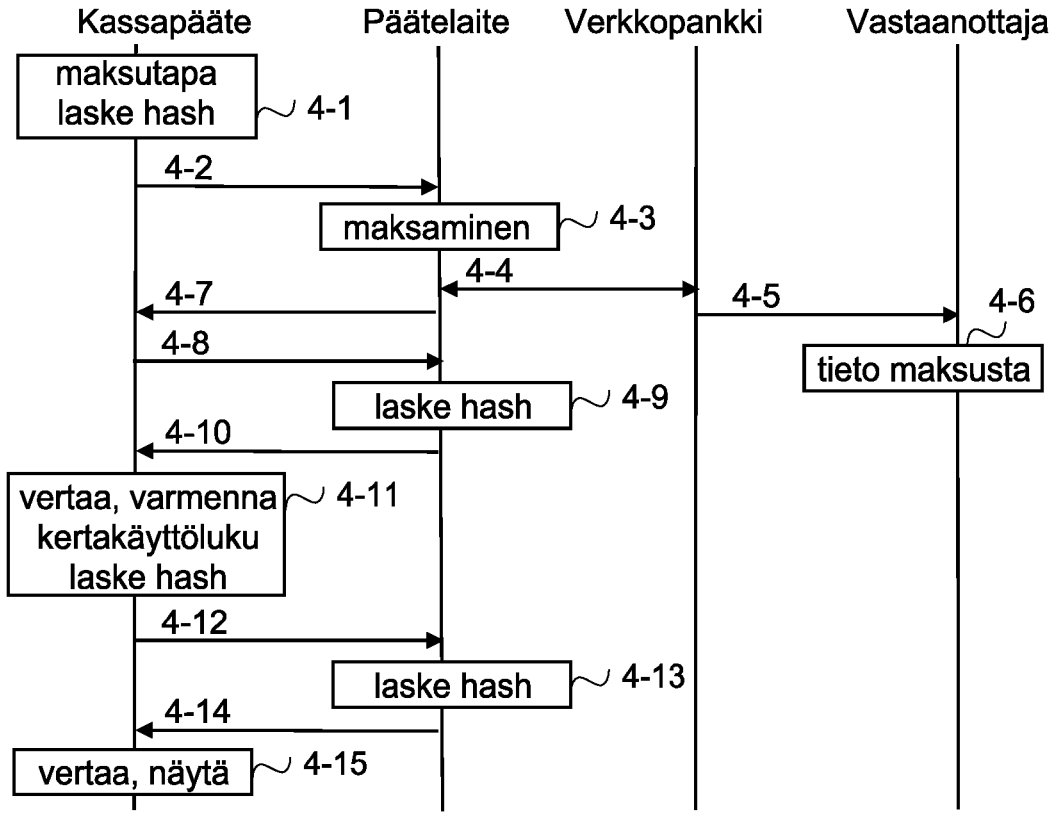


FIG.4

20165360 PRH 25-08-2016

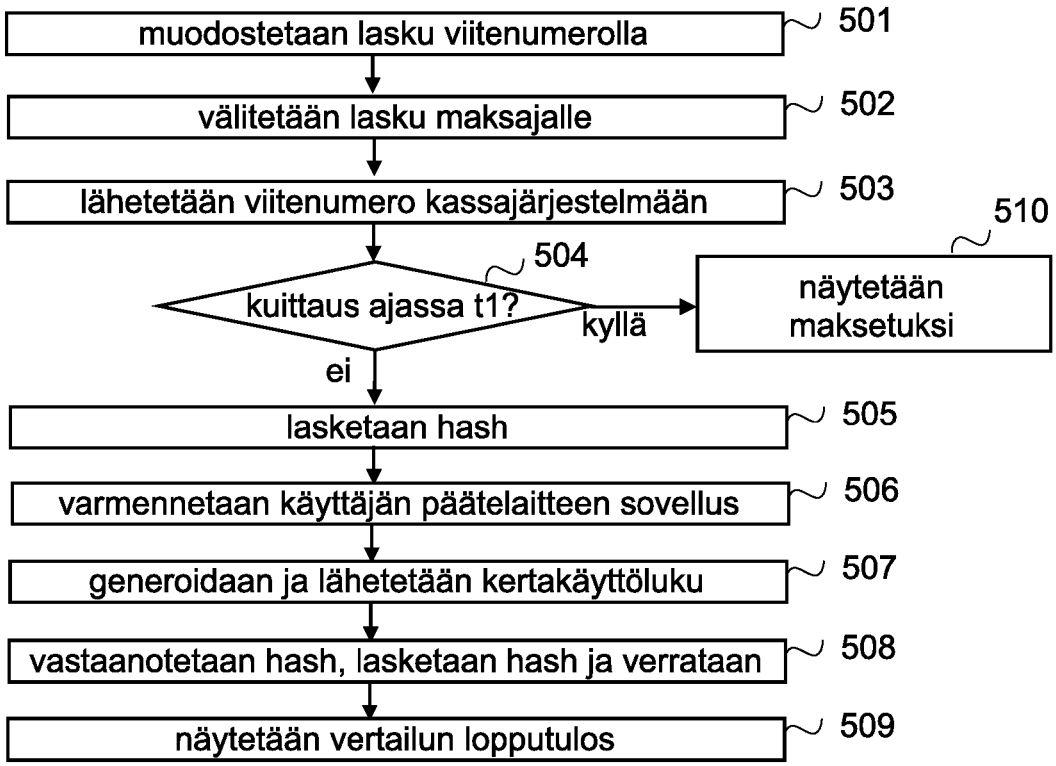


FIG.5A

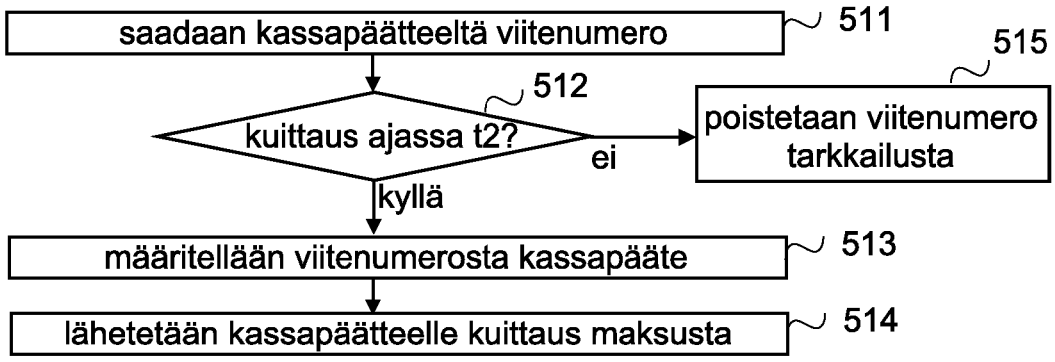


FIG.5B

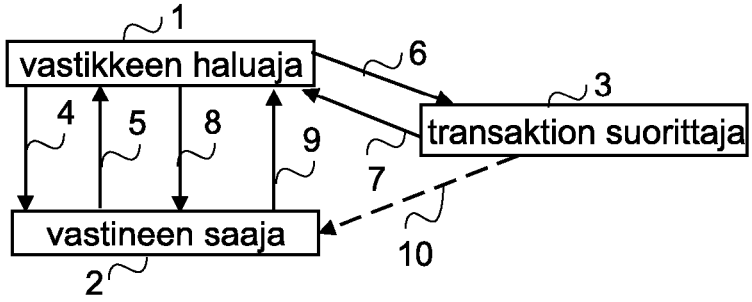


FIG.6

20165360 PRH 25-08-2016

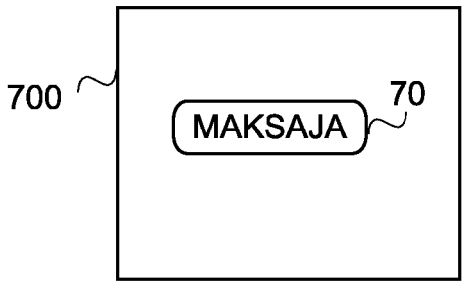


FIG.7A

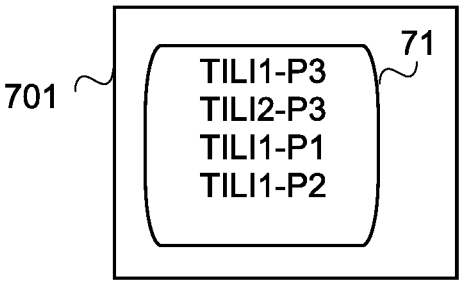


FIG.7B

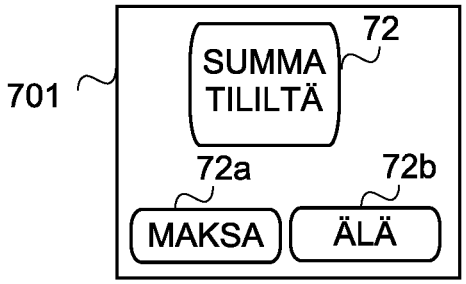


FIG.7C

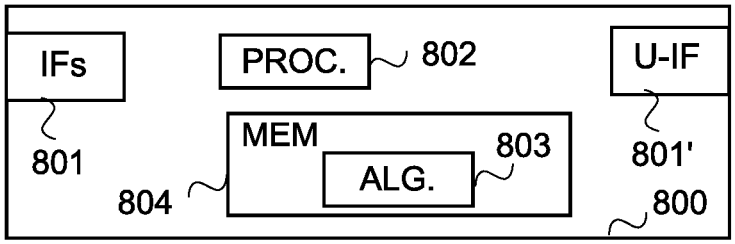


FIG.8

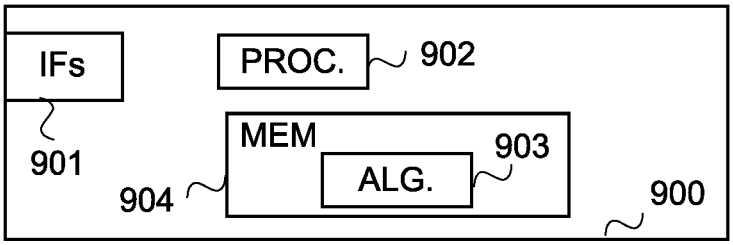


FIG.9

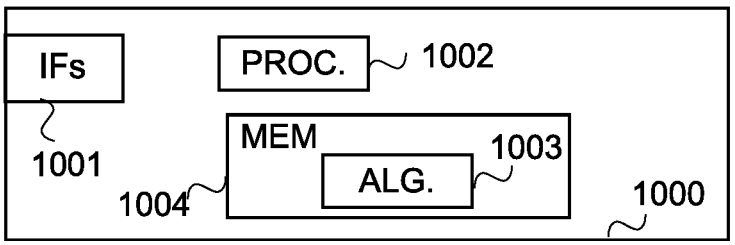


FIG.10

20165360 PRH 25-08-2016