Säker användaridentifiering

Tekniskt område

Föreliggande uppfinning avser ett system för säker identifiering av en användare. Uppfinningen avser också motsvarande metoder och tillhörande datorprogramprodukter.

Bakgrund

Uppfinningen avser i allmänhet problemet med att åstadkomma säker identifiering av en användare. Det är i sig välkänt att en digital identitet används för olika ändamål, exempelvis bankinloggning, inloggning på webbsidor, signering av betalningstransaktioner, signering av verkliga (butiks-) transaktioner, åtkomst till personliga digitala tjänster osv. Alla datoriserade tjänster som bygger på privat användarinformation lagrad på ett konto kräver och drar fördel av en säker inloggning eller signering för att komma åt den privata användarinformationen. Idag och i framtiden kommer fler digitala tjänster att vara tillgängliga utanför webben (www) och vara mer integrerade med det verkliga livet. Att numera flyga med ett flygbolag är ett exempel på en digital tjänst där det inte behövs någon förtryckt biljett.

Om man tar bankinloggning som ett exempel utnyttjar de gängse befintliga lösningarna en separat portabel autentiseringsenhet eller koddosa (exempelvis VASCO DIGIPASS, som används av de svenska bankerna SEB och Swedbank). En användare som vill logga in på sitt bankkonto kommer att använda en webbklient i en lokal enhet, såsom en handburen, bärbar eller stationär dator, för att besöka bankens webbplats och välja ett inloggningsformulär. Bankservern kommer att initiera en säker webbsession med den lokala enheten. För att fullborda upprättandet av den säkra webbsessionen kommer bankservern att kräva en säker identifiering av användaren. Användaren kommer därför att behöva mata in vissa personliga identifieringsdata i webbinloggningsformuläret, såsom hans personnummer. Användaren kommer vidare att mata in en PIN-kod på sin portabla koddosa tillsammans med åtminstone en kontrollkod som visas av bankservern i inloggningsformuläret på den lokala enheten. Som följd kommer den portabla koddosan att visa en slumpkod som användaren läser av och sedan matar in i inloggningsformuläret på den lokala enheten. Bankservern kommer att autentisera användaren genom att verifiera att den inmatade slumpkoden överensstämmer med

kontrollkoden och har alstrats av just den koddosa som tidigare förknippats med den aktuella användaren som har de personliga identifieringsdata som matats in.

Det finns flera nackdelar med denna tidigare kända lösning.

För det första måste användaren föra med sig och hålla reda på en separat enhet, dvs. den portabla koddosan, vilket är opraktiskt av logistiska skäl.

För det andra kräver lösningen flera steg med manuell interaktion från användaren. I exemplet ovan måste användaren först mata in sin PIN-kod på en miniknappsats på den portabla koddosan. En sådan aktivitet är exponerad för inmatningsfel orsakade av att användaren trycker ned någon annan knapp än den avsedda. Därefter måste användaren mata in sina personliga identifieringsdata i inloggningsformuläret. Efter detta måste användaren visuellt läsa den alstrade kontrollkoden på den lokala enhetens display och korrekt ange varje siffra i denna på den portabla koddosans knappsats – vilket åter är en aktivitet som är exponerad för inmatningsfel. Slutligen måste användaren läsa den alstrade slumpkoden på en liten, monokrom display på den portabla koddosan (vilket kan vara svårt, i synnerhet om de omgivande ljusförhållandena är dåliga, eller om användaren är en person med nedsatt synförmåga), och korrekt mata in varje siffra i slumpkoden i inloggningsformuläret på den lokala enheten.

Lösningen är för det tredje långt ifrån användarvänlig, eftersom den har konstruerats och dikteras uteslutande av tjänsteleverantören (banken) och inte av eller för användaren och hans behov av en bekväm lösning.

Det finns för det fjärde en säkerhetsfråga på grund av det faktum att kontrollkoden som användaren läser från den lokala enheten och matar in på sin koddosa måste vara begränsad i längd av praktiska skäl. Ju fler siffror i kontrollkoden, desto högre risk att användaren gör ett inmatningsfel genom att trycka ned fel knapp på koddosans knappsats. En mera komplex (exempelvis längre) kontrollkod skulle emellertid vara att föredra från ett datasäkerhetsperspektiv, eftersom detta skulle ge ett bredare kodrum som är svårare att knäcka.

Det finns för det femte ett problem med personlig integritet på grund av det faktum att användaren behöver avslöja sina personliga identifieringsdata, exempelvis hans personnummer, under inloggningsproceduren.

Föreliggande uppfinnare har insett att det finns utrymme för förbättringar med avseende på dessa problem, inte enbart vad gäller bankinloggningsexemplet som hänvisats till ovan, utan också när det gäller att tillhandahålla en säker identifiering av en användare i allmänhet.

Sammanfattning

Det är följaktligen ett syfte med föreliggande uppfinning att eliminera eller lindra åtminstone några av de problem som hänvisats till ovan.

Som en konceptuell idé bakom uppfinningen har föreliggande uppfinnare insett att de manuella steg som krävs av en användare för att säkert identifiera honom för en serverdel kan minskas påtagligt. Föreliggande uppfinnare har också insett att behovet av en separat portabel autentiseringsenhet eller koddosa kan elimineras. Istället kan uppfinningsmässig användning göras av en mobilterminal och dess unika identitet på ett telekommunikationsnät.

Denna konceptuella idé har förverkligats åtminstone i enlighet med de aspekter och utföringsformer av uppfinningen som hänvisas till nedan.

En aspekt av föreliggande uppfinning är därför ett system för säker identifiering av en användare, där systemet innefattar: en mobilterminal som är operativt ansluten till ett telekommunikationsnät och ett datanät; en lokal enhet som är operativt ansluten till datanätet; och en serverdel som innefattar åtminstone en server vilken är operativt ansluten till datanätet och åtminstone en server vilken är operativt ansluten till telekommunikationsnätet. Detta system kännetecknas av att serverdelen är konfigurerad att initiera en kommunikationssession med nämnda lokala enhet över nämnda datanät, där nämnda kommunikationssession har ett sessions-ID, att alstra en representation av sessions-ID:t samt att överföra representationen till den lokala enheten över nämnda datanät. Den lokala enheten är konfigurerad att presentera representationen i ett användargränssnitt på nämnda lokala enhet. Mobilterminalen är konfigurerad att registrera den presenterade representationen för att härleda nämnda sessions-ID, samt att sända ett meddelande innehållande det härledda sessions-ID:t till serverdelen över nämnda datanät. Serverdelen är vidare konfigurerad att bestämma en identitet hos mobilterminalen på telekommunikationsnätet, att verifiera den bestämda mobilterminalidentiteten mot förlagrade referensdata vilka kopplar samman mobilterminalidentiteten med privat användarinformation avseende nämnda användare, samt, efter framgångsrik verifiering, att förknippa nämnda kommunikationssession med nämnda privata användarinformation.

I en eller flera utföringsformer innefattas datanätet i internet eller är kompatibelt med detta. Den lokala enheten kan vara en dator som har en webbklientapplikation (såsom Internet Explorer, Mosaic, Netscape Navigator, Netscape Communicator, Opera, Mozilla Navigator, Mozilla Firefox, Safari eller Google Chrome). Kommunikations-

sessionen kan vara en säker webbsession (såsom en HTTPS-session ("Hypertext Transfer Protocol Secure") över TLS ("Transport Layer Security") eller SSL ("Secure Sockets Layer")). Uppfinningen är emellertid uttryckligen inte begränsad till enbart kommunikationssessioner av detta slag, vilket kommer att framgå tydligt av senare avsnitt av detta dokument.

Det skall understrykas att termen "sessions-ID" inte är begränsad till något särskilt format eller beskaffenhet inom ramen för föreliggande uppfinning. Vilken uppsättning data som helst är i princip kvalificerade som "sessions-ID", så länge den a) tjänar till att identifiera kommunikationssessionen för serverdelen, b) kan ingå i den representation som sänds till den lokala enheten, och c) kan härledas av mobilterminalen när den registrerat den presenterade representationen på den lokala enheten.

I en eller flera utföringsformer följer telekommunikationsnätet en eller flera standarder som valts från gruppen bestående av: GSM, UMTS, LTE, D-AMPS, CDMA2000, FOMA eller TD-SCDMA. Inom ramen för föreliggande uppfinning är dock omfånget för "telekommunikationsnät" inte begränsat till någon av dessa standarder. Tvärtom skall vilket nät som helst som kan förmedla kommunikation med eller mellan mobila enheter betraktas som ett "telekommunikationsnät", så länge nätet har intelligens som kan tilldela och detektera unika identiteter hos mobila enheter som ingår i nätet, samt som kan detektera när flera mobila enheter med samma identitet försöker komma åt nätet.

I en eller flera utföringsformer är mobilterminalen konfigurerad att, i meddelandet som innehåller det härledda sessions-ID:t och sänds på datanätet, inkludera information om den identitet som mobilterminalen har på telekommunikationsnätet. Serverdelen är konfigurerad att använda denna information som ingår i nämnda meddelande när den verifierar den bestämda mobilterminalidentiteten mot de förlagrade referensdata. Serverdelen baserar med andra ord sin autentisering av mobilterminalen både på identiteten hos mobilterminalen såsom den rapporterats i meddelandet över datanätet och på identiteten hos mobilterminalen såsom den detekterats på telekommunikationsnätet. Detta förhindrar illvilliga försök att använda någon annan mobilterminals identitet. Mobilterminalidentiteten kan exempelvis vara den IMSI ("International Mobile Subscriber Identity") som lagras på SIM-kortet i mobilterminalen, eller mobilterminalens hårdkodade IMEI ("International Mobile Equipment Identity"), eller väsentligen vilken förlagrad unik identitetsinformation som helst i mobilterminalen, som kan detekteras av telekommunikationsnätet och som inte kan manipuleras av en användare.

I en eller flera utföringsformer är serverdelen konfigurerad att alstra representationen av sessions-ID:t i form av grafiska bilddata, vilka innehåller en kodad version av sessions-ID:t och vilka kan presenteras visuellt på en display hos den lokala enheten. Dessa grafiska bilddata är med fördel en tvådimensionell streckkod såsom en Quick Response- (QR-) kod. Andra format för representationen av sessions-ID:t är emellertid möjliga i andra utföringsformer, inbegripande andra grafiska bildformat, men också icke-visuella format, såsom exempelvis ljudformat. Vilket dataformat som helst för representationen av sessions-ID:t är i princip lämpligt, under förutsättning att det i) kan överföras av serverdelen till den lokala enheten över datanätet, ii) kan presenteras av den lokala enheten i ett användargränssnitt hos densamma (såsom en bildskärm eller en högtalare), och iii) kan registreras av mobilterminalen (med användning av exempelvis en kamera eller en mikrofon) och bearbetas för att härleda det inkluderade sessions-ID:t.

En andra aspekt av uppfinningen är en metod för säker identifiering av en användare som har åtkomst till en mobilterminal vilken är operativt ansluten till ett telekommunikationsnät, och till en lokal enhet som är operativt ansluten till ett datanät. Metoden innefattar stegen, vid en serverdel som är operativt ansluten till nämnda datanät och nämnda telekommunikationsnät, att:

initiera en kommunikationssession över datanätet med den lokala enheten, varvid nämnda kommunikationssession har ett sessions-ID;

alstra en representation av sessions-ID:t i ett format som är lämpligt för presentation i den lokala enhetens användargränssnitt, i sin tur lämpligt att registreras av mobilterminalen vid presentation i nämnda användargränssnitt för att härleda det i nämnda representation inkluderade sessions-ID:t;

överföra representationen till den lokala enheten över nämnda datanät;

från mobilterminalen över nämnda datanät ta emot ett meddelande innehållande det härledda sessions-ID:t;

bestämma en identitet hos mobilterminalen på telekommunikationsnätet;

verifiera den bestämda mobilterminalidentiteten mot förlagrade referensdata som kopplar samman mobilterminalidentiteten med privat användarinformation avseende nämnda användare; samt

efter framgångsrik verifiering, förknippa nämnda kommunikationssession, som har det härledda sessions-ID:t, med nämnda privata användarinformation.

En tredje aspekt av uppfinningen är en datorprogramprodukt innefattande datorprogramkod för att utföra metoden enligt den andra aspekten av uppfinningen när nämnda datorprogramkod exekveras av en processor.

En fjärde aspekt av uppfinningen är en metod för säker identifiering av en användare som har åtkomst till en mobilterminal vilken är operativt ansluten till ett telekommunikationsnät, samt till en lokal enhet vilken är operativt ansluten till ett datanät. Metoden innefattar stegen, i nämnda mobilterminal, att:

registrera data som presenteras i den lokala enhetens användargränssnitt;

bearbeta de registrerade data för att härleda ett däri inkluderat sessions-ID, där sessions-ID:t representerar en kommunikationssession över datanätet mellan den lokala enheten och en serverdel;

sända ett meddelande innehållande det härledda sessions-ID:t till serverdelen över datanätet; samt

samarbeta med serverdelen för att möjliggöra bestämning av en identitet hos mobilterminalen på telekommunikationsnätet.

En femte aspekt av uppfinningen är en datorprogramprodukt innefattande datorprogramkod för att utföra metoden enligt den fjärde aspekten av uppfinningen, när nämnda datorprogramkod exekveras av en processor.

Utföringsformer av de andra till femte aspekterna av uppfinningen kan i allmänhet ha samma eller direkt motsvarande särdrag som något av de särdrag som hänvisats till ovan för den första aspekten.

Utföringsformer av uppfinningen har en fördel i att säker användaridentifiering åstadkoms på ett logistiskt förbättrat vis genom att eliminera behovet av en separat koddosa.

En annan fördel är att säker användaridentifiering kan göras effektivare, eftersom den manuella interaktion som krävs från användare har minskat.

Ytterligare en fördel är en förbättring vad gäller användarvänlighet.

Ännu en fördel är en förbättring i datasäkerhet, eftersom stegen med manuell användarinteraktion för att läsa en kontrollkod och mata in den på en koddosa har eliminerats, vilket lade en begränsning på komplexiteten hos kontrollkoden i känd teknik.

Det finns också en fördel vad gäller personlig integritet, eftersom användaren inte behöver röja några personliga identifieringsdata under inloggningsproceduren.

Kort beskrivning av ritningarna

Syften och särdrag hos samt fördelar med utföringsformer av uppfinningen kommer att framgå av den följande detaljerade beskrivningen, där hänvisning görs till de medföljande ritningarna, på vilka:

Fig. 1 är en översiktlig illustration av ett icke-begränsande exempel på ett system för säker identifiering av en användare, i vilket utföringsformer av föreliggande uppfinning kan utövas;

Fig. 2 är ett flödes- och signalschema som illustrerar några av de aktiviteter och meddelanden som utförs och utväxlas i systemet enligt fig. 1 vid utförande av en metod för säker identifiering av en användare; samt

Fig. 3 illustrerar ett användningsfall där en utföringsform av föreliggande uppfinning används för inloggning till en internet-bank.

Detaljerad beskrivning

Utföringsformer av uppfinningen kommer nu att beskrivas med hänvisning till de medföljande ritningarna. Uppfinningen kan, dock, utföras i många olika former och skall inte tolkas som att vara begränsad till de här angivna utföringsformerna; snarare ges dessa utföringsformer så att denna redogörelse kommer att vara genomarbetad och fullständig samt i sin helhet kommer att förmedla omfånget hos uppfinningen till fackmännen inom området. Den terminologi som används i den detaljerade beskrivningen av de ifrågavarande utföringsformer som illustrerats på de medföljande ritningarna är inte avsedd att vara begränsande för uppfinningen. På ritningarna avser likartade beteckningar likartade element.

Uppfinningen kommer först att beskrivas på en allmän nivå med hänvisning till ett system och en metod för säker identifiering av en användare som visas i figurerna 1 och 2. Därefter kommer några mera detaljerade utföringsformer och användningsfall att beskrivas.

Fig. 1 illustrerar ett system 1 för säker identifiering av en användare 2. Användaren 2 kommer att använda en lokal enhet 20 för att komma åt en tjänst som tillhandahålls över ett datanät 40 av en eller flera servrar 52a, 52b, 52n vid en serverdel 50. Tjänstens utförande är åtminstone delvis baserat på någon slags privat användarinformation 54 som avser användaren 2 och är lagrad i ett minne 55 som åtminstone en av servrarna 52a-52n har åtkomst till. Den privata användarinformationen 54 kan exempelvis avse ett bankkonto, en betalningstransaktion eller väsentligen vilken digital tillgång som helst som tillhör eller är förknippad med användaren 2. Tjänsten kan exempelvis vara bankinloggning, inloggning till någon annan webbtjänst, signering av transaktion, signering av transaktion i verkliga livet (som en VISA-kortbetalning), överföring av pengar mellan användare, eller användning av tjänsten som en elektronisk biljett.

Den lokala enheten 20 kan exempelvis vara en stationär, bärbar eller handburen dator som kör ett lämpligt klientoperativsystem och är försedd med programvara kapabel att kommunicera med användaren 2 genom ett användargränssnitt 22, samt även med serverdelen 50 över en kommunikationssession 42 på datanätet 40, för att utföra den begärda tjänsten. Servrarna 52a-52n kan på motsvarande vis vara ett godtyckligt antal serverdatorer eller serverdatorgrupper som kör lämpligt/lämpliga serveroperativsystem och är kapabla att tillhandahålla den begärda tjänsten åt användaren 2 över kommunikationssessionen 42 på datanätet 40.

Användaren 2 har också tillgång till en mobilterminal 10, exempelvis en mobiltelefon, smartphone eller personlig digital assistent (PDA). I enlighet med uppfinningen spelar mobilterminalen 10 en aktiv roll vid den säkra identifieringen av användaren 2. Utöver detta kan användaren 2 givetvis använda sin mobilterminal 10 för att genomföra röstsamtal med andra användare vilka kan nås genom ett telekommunikationsnät 30. Förutom röstsamtal kan användaren 2 använda diverse andra telekommunikationstjänster, såsom internet-surfning, videosamtal, datasamtal, faxsändningar, stillbildsändningar, videosändningar, elektroniska meddelanden samt e-handel. Ingen av dessa telekommunikationstjänster är emellertid central vad gäller föreliggande uppfinning; det finns inga begränsningar till någon särskild uppsättning tjänster i detta avseende.

Mobilterminalen 10 ansluter till telekommunikationsnätet 30 över en radiolänk 34 och en basstation 32. Mobilterminalen 10 och telekommunikationsnätet 30 kan följa någon kommersiellt tillgänglig mobiltelekommunikationsstandard, inbegripande men ej begränsat till GSM, UMTS, LTE, D-AMPS, CDMA2000, FOMA samt TD-SCDMA. Ett konventionellt fast telenät (PSTN, "Public Switched Telephone Network") med diverse stationära telefonterminaler kan vara förbundet med telekommunikationsnätet 30.

Den funktionalitet som utförs i systemet 1 för att åstadkomma säker identifiering av användaren 2 kan sammanfattas som följer. När tjänsten begärs av användaren 1, kan inledningsvis en begäran sändas från den lokala enheten 20 till serverdelen 50 (se steg 202 i fig. 2). Som följd kommer kommunikationssessionen 42 att etableras mellan serverdelen 50 och den lokala enheten 20. Kommunikationssessionen 42 kommer att tilldelas ett sessions-ID, se steg 204 i fig. 2. Kommunikationssessionen 42 kan exempelvis vara en säker webbsession (såsom HTTPS TLS eller SSL) mellan en webbklient i den lokala enheten 20 och en webbserver vid serverdelen 50, men andra typer av kommunikationssessioner är också möjliga. Noterbart är, dock, att kommunika-

tionssessionen 42 vid detta tillfälle inte kommer att vara kopplad till någon särskild användare, till skillnad från de tidigare kända tillvägagångssätten som hänvisats till i avsnittet Bakgrund i detta dokument, och inte heller kommer den att vara kopplad till någon privat användarinformation vid serverdelen 50. Vid detta tidiga skede kommer istället sessionen 42 att vara säker men anonym i den meningen att serverdelen 50 är omedveten om den användare eller privata användarinformation som den skall förknippas med.

För att kunna bestämma vem som sessionen 42 avser samt åstadkomma en autentiserad session, vidtas följande åtgärder. I steg 206 alstrar serverdelen 50 en representation av sessions-ID:t för kommunikationssessionen 42. Representationen har med fördel formen av grafiska bilddata, företrädesvis en tvådimensionell streckkod såsom en Quick Response- (QR-) kod. Andra alternativ för den i steg 206 alstrade representationen är emellertid också möjliga, vilket har förklarats ovan i avsnittet Sammanfattning. I steg 208 överför serverdelen 50 representationen av sessions-ID:t över datanätet 40 till den lokala enheten 20, som visas vid 209. Överföringen 209 kan göras i enlighet med någon standard eller något protokoll som är tillämpbar(t) för den ifrågavarande typen av kommunikationssession. När sessionen 42 exempelvis är en webbsession och representationen är en QR-kod, kan överföringen 209 inbegripa att kapsla in QR-koden i html- eller xml-kod som läses av den lokala enheten 20 från serverdelen 50. Vid mottagning av den överförda representationen vid den lokala enheten 20, kommer den lokala enheten 20 att presentera den mottagna representationen av sessions-ID:t i sitt användargränssnitt 22. Som fortsättning på det ovan givna exemplet kan detta inbegripa att använda en webbklientapplikation i den lokala enheten 20 för att rendera den mottagna html- eller xml-koden och presentera den inkapslade QR-koden, som visats vid 24 i fig. 1, på en displayenhet som är del av användargränssnittet 22.

Användaren 2 kan nu använda sin mobilterminal 10 för att fortsätta med sin säkra identifiering för serverdelen 50. I ett steg 212 kommer användaren 2 inledningsvis att starta en applikation för säker identifiering i sin mobilterminal och logga in, exempelvis genom att ange en PIN-kod. Applikationen för säker identifiering kan exempelvis vara en Java-applet eller –midlet, eller någon annan slags exekverbar programvara som är skriven i ett lämpligt programmeringsspråk vilket är kompatibelt med mobilterminalens operativsystem. Applikationen ansvarar för att utföra eller styra de väsentliga delarna av funktionaliteten i mobilterminalen, som visas i fig. 2.

I steg 214 kommer användaren 2 således att använda sin mobilterminal för att registrera representationen 24 som presenteras i den lokala enhetens användargränssnitt 22. I den skildrade utföringsformen där representationen är i form av en grafisk QR-kod, kommer registreringen att göras genom att ta ett fotografi av den visade QR-koden 24 med hjälp av en kamera 12 som ingår i mobilterminalen 10. Fotografiet kan utsättas för bildförbehandling, om så är lämpligt, för att förbättra läsligheten av dess innehåll. Mobilterminalen kommer därefter att bearbeta den representation som ingår i bilden genom lämpliga objektigenkänningsalgoritmer för att härleda sessions-ID:t.

I steg 216 kommer mobilterminalen 10 att komponera ett meddelande 217 som innehåller det härledda sessions-ID:t från steg 214. Meddelandet 217 kommer att sändas till serverdelen 50 över en lämplig kommunikationskanal, såsom en TLS- eller SSL-anslutning över datanätet 40. Meddelandet 217 innehåller också en identifierare för mobilterminalen på telekommunikationsnätet 30, exempelvis dess IMSI- eller IMEI-nummer. Det härledda sessions-ID:t, och möjligen annat innehåll i meddelandet 217, krypteras med fördel med en i mobilterminalen 10 lagrad krypteringsnyckel. Vilken öppen eller företagsägd krypteringsstandard som helst kan användas för sådan kryptering, inbegripande men ej begränsat till AES ("Advanced Encryption Standard", avancerad krypteringsstandard) eller DES ("Digital Encryption Standard", digital krypteringsstandard). Krypteringsnyckeln kan exempelvis ha tagits emot i mobil-terminalen i samband med anförskaffande och installation av applikationen för säker identifiering i mobilterminalen 10.

På serverdelen 50 tas meddelandet 217 emot i steg 218 över datanätet 40. Meddelandet analyseras för att bestämma den däri ingående mobilterminalidentifier-aren. När kryptering har tillämpats, kan serverdelen 50 använda förlagrade referensdata 56 i en säker databas 57 för att hämta en dekrypteringsnyckel som är lämplig för den ifrågavarande mobilterminalen 10, som den identifierats genom mobilterminalidentifier-aren. En sådan dekrypteringsnyckel kan ha lagrats i de förlagrade referensdata 56 i samband med mobilterminalens 10 anförskaffande och installation av applikationen för säker identifiering. Efter dekrypteringen, om sådan tillämpas, bestäms det i meddelandet 217 ingående härledda sessions-ID:t i steg 218.

För att kunna verifiera att meddelandet 217 med sitt härledda sessions-ID verkligen härstammar från mobilterminalen 10 och inte från någon annan mobilterminal som illvilligt försöker uppträda som mobilterminalen 10, bestämmer serverdelen i steg 219 identiteten hos mobilterminalen 10 också via telekommunikationsnätet 30. Server-delen 50 använder med andra ord den inneboende säkra och icke-publika beskaffen-

heten hos telekommunikationsnätet 30 för att verifiera att mobilterminalens 10 IMSI, IMEI, etc., som rapporterats i meddelandet 217 över datanätet 30, är samma som det IMSI, IMEI, etc., som detekterats för mobilterminalen 10 på telekommunikationsnätet 30.

Bestämningen i steg 219 av identiteten hos mobilterminalen 10 på telekommunikationsnätet 30 kan för detta ändamål göras genom ett meddelande såsom ett data-SMS eller ett MMS som skickas från mobilteminalen 10 (se steg 221 i fig. 2) till en telekommunikationsserver som ingår bland servrarna 52a-52n. Serverdelen 50 kan hämta identiteten (dvs. IMSI) hos mobilterminalen 10 från huvudavsnittet i detta SMS- eller MMS-meddelande. Alternativt kan bestämningen i steg 219 inledas med att serverdelen 50 skickar en utmaningsbegäran i ett meddelande såsom ett data-SMS eller ett MMS till mobilterminalen 10 över telekommunikationsnätet 30. Vid mottagning kan mobilterminalen 10 alstra och sända ett utmaningssvar över en säker anslutning på datanätet 40 till serverdelen 50 i steg 221. Endast den riktiga mobilterminalen 10 kommer att ta emot utmaningsbegäran över telekommunikationsnätet 30; när serverdelen 50 tar emot utmaningssvaret, vet den därför att det måste ha kommit från den riktiga mobilterminalen 10 och har därför indirekt bestämt mobilterminalens 10 identitet på telekommunikationsnätet 30.

Istället för att sända ett meddelande kan bestämningen av identiteten hos mobilterminalen 10 på telekommunikationsnätet 30 inbegripa att göra ett datasamtal i steg 221 från mobilterminalen 10 till telekommunikationsservern. Vid mottagning av det inkommande datasamtalet i steg 219, kan telekommunikationsservern bestämma identiteten hos terminalen 10 som nummerpresentation CID ("Caller Identification"), CLID ("Calling Line Identification"), CNID ("Calling Number Identification"), osv., beroende på implementation.

Som ytterligare alternativ kan serverdelen 50 använda andra inneboende egenskaper hos telekommunikationsnätet 30 för att bestämma identiteten hos mobilterminalen 10 på telekommunikationsnätet 30. Detta kan, exempelvis, inbegripa användande av systemdatabaser som är integrerade delar av telekommunikationsnätet 30, såsom ett HLR-register ("Home Location Register") eller VLR-register ("Visiting Location Register"), i vilket IMSI och IMEI hos mobilterminaler i nätverket 30 ingår. Detta kan kombineras med bestämning av cell-ID för den cell i nätverket 30 som terminalen 10 för närvarande befinner sig i, samt kontroll mot ett självrapporterat cell-ID som del av meddelandet 217 över datanätet 40. Fackmannen kommer att inse att det finns många

möjligheter att bestämma den sanna identiteten hos en mobilterminal på ett telekommunikationsnät, och uppfinningen är inte begränsad till något särskilt sätt.

När identiteten hos mobilterminalen 10 på telekommunikationsnätet 30 har bestämts i steg 219, kan serverdelen 50 i steg 220 verifiera att denna identitet är samma som den mobilterminalidentifierare som rapporterats i meddelandet 217 över datanätet 30. Om applikationen för säker identifiering kopieras till andra enheter eller datorer än den sanna mobilterminalen 10, eller om en kommunikation påbörjas av någon som simulerar applikationen, kommer serverdelen 50 att veta att kommunikationen inte sänts av den sanna mobilterminalen 10. Även om kommunikationen som sänts av intrångsgöraren kommer att simulera all information som skickas genom datanätet 40 (där serverdelen 50 kan misslyckas med att detektera att data sänts av någon annan än den sanna användaren 2 på datanätet 40), kommer serverdelen 50 hursomhelst att detektera att applikationen inte kommunicerar med användning av den sanna mobilterminalen på telekommunikationsnätet 30. Serverdelen 50 kommer därför att veta att kommunikationen inte sänts av den verifierade hårdvaran.

I steg 220 kommer vidare den bestämda mobilterminalidentiteten att verifieras mot de förlagrade referensdata 56 som kopplar samman mobilterminalidentiteten med den privata användarinformationen 54 som avser användaren 2 och är lagrad i minnet 55. Efter framgångsrik verifiering i steg 220 kan den i steg 204 skapade kommunikationssessionen 42 förknippas med den privata användarinformationen 54 för användaren 2 i ett efterföljande steg 222. Detta kan göras genom användning av sessions-ID:t, vilket tilldelades kommunikationssessionen 42 i steg 204 och vilket också är tillgängligt i meddelandet 217 som rapporterats från mobilterminalen 10 till serverdelen 50 efter registrering av representationen av sessions-ID:t på den lokala enheten 20. Som ett resultat av steg 222 har den säkra kommunikationssessionen 42 nu blivit en autentiserad session, se steg 224, i den meningen att den nu är förknippad vid serverdelen 50 med den ifrågavarande användaren 2 och hans privata användarinformation 54.

Den procedur för säker användaridentifiering som beskrivits ovan kräver anförskaffande och installation av en applikation för säker identifiering i mobilterminalen. I utföringsformer av uppfinningen kan detta göras på ett säkert och ändå bekvämt vis på följande sätt. Användaren 2 kommer först att till sin mobilterminal 10 ladda ner den programvara som kommer att utgöra applikationen för säker identifiering. Detta kan göras på konventionellt vis, exempelvis i en webbsession, en FTP-session, som en bilaga till ett e-postmeddelande, över ett seriellt gränssnitt såsom USB osv. Alternativt kan det exempelvis göras genom att skanna en QR-kodad version av programvaran som

presenteras exempelvis vid en webbplats och tolka den inskannade QR-koden som programvarukod.

Den på så vis erhållna programvaran kommer sedan att installeras i mobilterminalen 10. Användaren 2 kan med fördel uppmanas att ställa in en PIN-kod att användas för efterföljande användningar av applikationen för säker identifiering (exempelvis i inloggningssteget 212 i fig. 2).

Under installationen, eller den första gången applikationen körs, kommer användaren 2 att uppmanas att etablera en säker webbsession mellan den lokala enheten 20 och serverdelen 50 över datanätet 40. När serverdelen 50 är en internet-bank, kan användaren 2 presenteras inför en väsentligen konventionell inloggningsskärmbild, där användaren 2 ombeds ange sina personliga identifieringsdata, läsa en presenterad kontrollkod och mata in den på sin koddosa, och därefter ange den slumpkod som alstras av koddosan – i mångt och mycket som i det tidigare kända tillvägagångssätt som beskrivits i avsnittet Bakgrund i detta dokument. Till skillnad från det tidigare kända tillvägagångssättet kommer dock serverdelen 50 att alstra en QR-kod och visa den på den lokala enheten 20. Användaren 2 kommer att uppmanas att skanna QR-koden med användning av den inbyggda kameran i hans mobilterminal 10.

Mobilterminalen 10 kommer att svara till serverdelen 50 i en handskakningsoperation, i vilken den inskannade QR-koden sänds tillsammans med en identifierare (exempelvis IMSI, IMEI) för mobilterminalen 10 över datanätet 30. Som följd, i implementationer där kryptering används för utväxlingen av information i stegen 216-218 i fig. 2, kommer serverdelen 50 att svara med en krypteringsnyckel för lagring i lokalt och företrädesvis säkert minne i mobilterminalen 10. Serverdelen 50 kan också verifiera den mottagna mobilterminalidentifieraren genom att bestämma identiteten hos mobilterminalen 10 på telekommunikationsnätet 30 på väsentligen samma sätt som har beskrivits ovan med hänvisning till stegen 219-221 i fig. 2. Efter framgångsrik verifiering kan serverdelen 50 infoga eller uppdatera en post i de förlagrade referensdata 56 för att skapa en länk mellan användaren 2, identiteten hos hans mobilterminal 10 och hans privata användarinformation 54. Från och med nu behöver användaren 2 inte längre använda sin koddosa för att logga in till sin internet-bank (osv.); han kan istället bekvämt logga in genom att använda sin mobilterminal och registrera QR-koder med den inbyggda kameran.

Fig. 3 illustrerar ett användningsfall där användaren 2 drar fördelaktig nytta av den föreliggande uppfinningen vid inloggning till sin internet-bank från en lokal enhet 20. I den i fig. 3 visade situationen har användaren 2 redan begärt en säker webbsession

med bankservern vid serverdelen 50 genom att exempelvis klicka på en länk "Inloggning med min telefon" på hemsidan för internet-banken ifråga. Stegen 202 och 204 i fig. 2 har med andra ord redan utförts. Som följd initierar bankservern kommunikationssessionen 42 och tilldelar dess sessions-ID. Se även steg 204 i fig. 2. Bankservern alstrar också representationen av sessions-ID:t i form av en QR-kod 24 samt överför den till den lokala enheten 20. Vid mottagning presenterar den lokala enheten 20 QR-koden 24 i sitt användargränssnitt 22. Se steg 206-210 i fig. 2. Eventuellt uppmanad av ett meddelande i användargränssnittet 22 på den lokala enheten 20, eller helt enkelt utlöst av förekomsten av QR-koden 24, vänder sig användaren 2 till sin mobilterminal 10 och startar applikationen för säker identifiering, se steg 212 i fig. 2. Detta illustreras vid den vänstra fyllda cirkeln "1" i fig. 3. Användaren 2 anger också sin PIN-kod i användargränssnittet på mobilterminalen 10.

Som illustreras vid den mittersta fyllda cirkeln "2" i fig. 3 skannar användaren 2 QR-koden 24 genom att använda den inbyggda kameran 12 i denna mobilterminal för att registrera en bild (fotografi). Det som nu följer är stegen 214 till och med 222 i fig. 2, som slutar med en framgångsrik autentisering av kommunikationssessionen 42 i steg 224. Detta innebär också att användaren 2 har loggat in till sitt bankkonto som representeras av hans privata användarinformation 54 vid bankservern. Se den högra fyllda cirkeln "3" i fig. 3.

Detta användningsfall illustrerar ytterst väl vissa av uppfinningens förtjänster, tack vare enkelheten och bekvämligheten i den interaktion som utförs av användaren 2. Diverse andra användningsfall är emellertid lika möjliga inom ramen för uppfinningen. Ett sådant alternativt användningsfall är exempelvis när användaren 2 redan har loggat in på sin internet-bank och nu vill signera en banktransaktion, såsom betalning av en faktura genom en giroöverföring. Proceduren är väldigt likartad; när det är dags att begära en signatur för transaktionen från användaren 2, kommer bankservern att initiera en säker session för transaktionen; en QR-kod som representerar sessions-ID:t för denna session kommer att överföras till den lokala enheten 20 och visas på dess display; användaren 2 kommer att skanna QR-koden med sin mobilterminal 10; och, till slut, kommer serverdelen 50 att betrakta transaktionssessionen som autentiserad och, i praktiken, transaktionen som vederbörligen signerad av användaren 2.

Ett liknande alternativt användningsfall är inloggning till andra webbtjänster eller konton än sådana som har att göra med internet-banker. Väsentligen samma process används för inloggning till sådana andra webbtjänster eller konton.

Ytterligare ett alternativt användningsfall är betalning i samband med e-handel. En användare besöker en butik på en internet-webbplats och vill fullborda ett köp. Internet-butiken begär ett ID från en ID-server som ingår bland servrarna 52a-52n vid serverdelen 50. Användaren använder sin mobilterminal och skannar QR-koden som presenteras i webbläsaren. Den presenterade QR-koden inbegriper information om ID:t. Användarens applikation i mobilterminalen sänder det inskannade ID:t till ID-servern. ID-servern känner nu till vem som skannade QR-koden. Den tar också emot information från telekommunikationsnätet vilken berättar för servern att applikationen fortfarande kör på den registrerade mobilterminalen. Om den är ansluten till användarens bank eller bankkonto, kan ID-servern nu dra pengar från användaren. ID-servern sänder därefter information till internet-butiken avseende den fullbordade transaktionen. Internet-butiken kan slutligen presentera information om den framgångsrika betalningen och fullborda köpet.

Ytterligare ett annat alternativt användningsfall är betalning i verkliga livet. Tillvägagångssättet som uppfinningen tillhandahåller kan tillämpas även på betalningar i verkliga livet. Kassapparaten eller –terminalen fungerar som den lokala enheten och presenterar en QR-kod. Det finns nu en kommunikationssession i form av en "kassa-apparat – server"-session istället för en webbsession.

Metoden som beskrivits ovan med hänvisning till fig. 2 kan utföras som en datorprogramprodukt innefattande datorprogramkod för att utföra de delar av metoden som avser serverdelen när datorprogramkoden exekveras av en processor, exempelvis implementerad i någon av servrarna 52a-52n i fig. 1. Metoden kan också utföras som ett datorläsbart medium på vilket det finns lagrat ett datorprogram innefattande dator-programkod för att utföra metoden när datorprogramkoden exekveras av en processor. Processorn kan åter exempelvis implementeras i någon av servrarna 52a-52n i fig. 1. Det datorläsbara mediet kan exempelvis vara något av minnena 55, 57 i fig. 1, eller något annat lämpligt medium, inbegripande men ej begränsat till en optisk skiva (exempelvis CD eller DVD), ett portabelt halvledarminne (exempelvis ett USB-minne), en magnetisk skiva, eller en filserver som är åtkomlig i ett datornät såsom internet.

Metoden som beskrivits ovan med hänvisning till fig. 2 kan vidare utföras som en datorprogramprodukt (exempelvis en telefon-app) innefattande datorprogramkod för att utföra de delar av metoden som avser mobilterminalen när datorprogramkoden exekveras av en processor i mobilterminalen 10. Metoden kan också utföras som ett datorläsbart medium på vilket det finns lagrat ett datorprogram innefattande dator-programkod för att utföra metoden när datorprogramkoden exekveras av en processor i

mobilterminalen 10. Det datorläsbara mediet kan vara något lämpligt medium, inbegripande men ej begränsat till en optisk skiva (exempelvis CD eller DVD), ett portabelt halvledarminne (exempelvis ett USB-minne), en magnetisk skiva, eller en filserver som är åtkomlig i ett datornät såsom internet.

Uppfinningen har beskrivits ovan i detalj med hänvisning till utföringsformer av densamma. Enligt vad som enkelt inses av fackmännen inom området är emellertid andra utföringsformer lika möjliga inom ramen för uppfinningen, såsom denna definieras av de bifogade patentkraven.