(12) **PATENT**

(19) NO (11) **337813** (13) **B1**

NORGE (51) Int Cl.

G06Q 20/30 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/16 (2012.01)
G06Q 20/16 (2012.01)

Patentstyret

(21)	Søknadsnr	20140098	(86)	Int.inng.dag og søknadsnr
(22)	Inng.dag	2014.01.28	(85)	Videreføringsdag
(24)	Løpedag	2014.01.28	(30)	Prioritet
(41)	Alm.tilgj	2015.07.29		
(45)	Meddelt	2016.06.27		

(73)	Innehaver	Protectoria AS, Postboks 1208 Vika, 0110 OSLO, Norge
(72)	Oppfinner	Trond Lemberg, Skotbuveien 81, 1409 SKOTBU, Norge
(74)	Fullmektig	Oslo Patentkontor AS, Postboks 7007 Majorstua, 0306 OSLO, Norge

(54) Benevnelse **Fremgangsmåte for sikring av en elektronisk transaksjon**

(56) Anførte publikasjoner
US 20040153655 A1
US 2013204786 A1

(57) Sammendrag

Fremgangsmåte for å sikre en elektronisk transaksjon mellom en applikasjonsserver og en sluttbruker, hvor nevnte sluttbruker har tilgang til en telefon og en datamaskin med en høyttaler.

Teknisk felt

Den foreliggende oppfinnelsen vedrører et system og en fremgangsmåte for å sikre en elektronisk transaksjon, og mer spesielt et system og en fremgangsmåte for å sikre en elektronisk transaksjon mellom en applikasjonsserver og en sluttbruker.

Bakgrunn for oppfinnelsen

Det har blitt klart at tradisjonelle sikkerhetsløsninger ikke lenger er i stand til å beskytte transaksjoner fra å bli manipulert av uvedkommende. På grunn av mangel på effektive og sterke sesjonssikkerhetsmekanismer utplassert i vanlig brukte sluttbrukersystemer, har «Man-in-the-middle» angrep hele tiden blitt enklere å utføre, og blir også mer og mer sofistikerte og skalerbare.

Som en konsekvens, har det å stjele penger fra bankene og deres kunder ved å manipulere betalings- og pengeoverføringstransaksjoner, manipulere elektroniske avtaler og mest sannsynlig også manipulere børstransaksjoner over usikre nettverk og enheter, etc. blitt et stort problem for folk, bedrifter og til og med hele nasjoner.

Teoretisk ville «Public Key Infrastruktur» være en god teknologisk kandidat for å beskytte transaksjoner, men frekvensen av utplasseringer i markedet er relativt liten på grunn av store kostnader, tung logistikk og med en generell mangel på interoperabilitet mellom heterogene distribusjoner.

US 20040153655 A1 beskriver en 'verbal feedback' over en telefonkanal fra sluttbruker til mekanismen/tjenesten. Det forklares dessuten at tjenesten spesifikt er et dokumentsigneringssystem som gjør bruk av telefoni-kanalen for å informere sluttbruker om dokumentinnhold, og som i retur krever at sluttbruker sier noe som bekrefter/avkrefter avtalen.

US 2013204786 A1 forutsetter at sluttbruker overfører et identifiserende bilde til mekanismen/tjenesten. Videre sies det at transaksjonen er begrenset til finansielle transaksjoner. Bildeoverføringsmekanismen benyttes for å la sluttbruker autorisere en transaksjon basert på at man matcher det overførte bildet med et mønster man på forhånd besitter i mekanismen.

US 20040153655 A1 og US 2013204786 A1 beskriver altså to alternativer for verifikasjon av en bruker ved benyttelse av to kommunikasjonskanaler. Det benyttes her ytterligere sikkerhetsnivåer slik som stemmegjenkjenning (D1) og et identifiserende bilde (D2).

Problemet med disse løsningene er at samme hemmelighet for verifikasjon benyttes hver gang og at denne hemmeligheten deles mellom alle parter på usikrede linjer.

Sammenfatning av oppfinnelsen

Det er derfor formålet med den foreliggende oppfinnelse, slik angitt i kravsettet, å løse problemene som er nevnt ovenfor.

Foreliggende oppfinnelse beskriver en fremgangsmåte for å sikre en elektronisk transaksjon mellom en applikasjonsserver og en sluttbruker, hvori sluttbruker har tilgang til en telefon og en datamaskin med en høyttaler, applikasjonsserveren sender en verifikasjon til en transaksjonsverifikasjonsserver hvor:

- transaksjonsverifiseringsserveren konverterer verifikasjonen i minst to lydfiler,
- transaksjonsverifiseringsserveren setter opp en samtale til sluttbruker og spiller av den første lydfilen på telefonen til sluttbruker i henhold til parametere og transaksjonsopplysningen beskrevet i verifiseringsordren,
- hvis sluttbrukeren aksepterer transaksjonsdetaljene presentert som en syntetisk stemme i det aktuelle språket i løpet av telefonsamtalen, spiller transaksjonsverifiseringsserveren av den andre lydfilen som en utgående lyd-stream på sluttbrukerens datamaskinhøyttaler,
- den andre lydfilen registreres av mikrofonen på sluttbrukerne telefonen,
- den innspilte andre lydfilen blir overført fra mikrofonen på telefonen til transaksjonsverifikasjonsserveren via selve telefonsamtalen,
- transaksjonsverifiseringsserverens sammenlikner den utgående streamede andre lydfilen med den mottatte andre lydfilen, og
- om de samstemmer, sender transaksjonsverifikasjonsserveren en positiv kvittering til applikasjonsserveren,
- en negativ kvittering sendes til applikasjonsserveren i tilfelle sluttbruker ikke aksepterer transaksjonsdetaljene presentert av mekanismen ved å avslutte samtalen eller trykke på en knapp på telefonen, i tilfelle transaksjonsverifiseringsserveren ikke er i stand til å finne en likhet mellom utgående streamet lyd med den innkommende mottatte lyden, en negativ kvittering sendes til applikasjonsserveren.

Fremgangsmåten løser de ovenfor nevnte problemer ved å sikre en elektronisk transaksjon mellom en applikasjonsserver og en sluttbruker. Dette gjøres uten å dele noen hemmeligheter mellom alle parter over usikret utstyr, miljøer eller nettverk.

Fremgangsmåten gjør det mulig for sluttbrukeren å verifisere en elektronisk transaksjon mot en applikasjonsserver, ut av rekkevidde av kriminelle eller andre uvedkommende, uten å kreve noen annen forutsetning fra sluttbrukerens side enn å være i stand til å ta en telefonsamtale innen nærhet til en datamaskin med en fungerende høyttaler koblet til et nettverk.

Detaljert beskrivelse

Mekanismen i henhold til oppfinnelsen virker i henhold til denne beskrivelsen:

1) En applikasjons server genererer en transaksjonshemmelighet koblet til denne transaksjonsbekreftelsesmetoden. Årsaken kan være at applikasjonen er trigget av en risikoparameter, enten i programmet eller levert av en annen kilde. Når du har generert den opprinnelige transaksjonshemmeligheten, genererer programmet en proxy-hemmelighet (PS) som korrelerer til opprinnelsestransaksjonens hemmelighet, typisk et tilfeldig tall eller kryptografisk gjort fingeravtrykk, som en hash verdien av transaksjonshemmeligheten.

2) Applikasjonsserveren genererer og sender deretter en verifiseringsordre (VO) til Transaksjons-Verifiserings-Serveren (TVS).

3) TVS er enten direkte eller indirekte forbundet med minst en teleoperatør (F.eks. via en SIP-stamme og muligens et ISUP grensesnitt) eller koblet til applikasjonsserveren og dens IP-nettverk over en sikker tilkobling.

4) VO har minimum et troverdig telefonnummer, ordrenummer, PS, transaksjonsdetaljer og en språkindikator. I tillegg kan VO eventuelt inkludere flere kontrollindikatorer (KI) og krav til hver av dem, for eksempel Identifikasjons-Indikatorer (II) som skal benyttes som del av transaksjonsverifiseringsmekanismen, oppringningskontrollindikatorene (CCI) eller posisjonsindikatorene (PI) som skal brukes før transaksjonsverifiseringsmekanismen blir startet

a. Krav til (II) kan ved hjelp av et integrert stemmebiometrisystem, en annen type biometrisystem, PKI-system, DTMF basert autentiseringsmetode f.eks. fra et telefonbasert banksystem, eller lignende, der sluttbrukeren allerede er registrert. Som et underkrav for (II) kan det settes

kvalitetsparametere avhengig av et risikonivå for den spesielle transaksjonen som skal sikres, f.eks. for en middels risiko transaksjon skal stemmebiometrisystemet identifisere sluttbrukeren ved å kreve sluttbrukeren å bare si navnet sitt eller en avtalt setning som forespurt i samtalen fra TVS, mens for høy-risiko-transaksjon må brukeren også gjenta et unikt tilfeldig tall hentet fra VO og opprinnelig gitt til sluttbruker via syntetisk stemme generert av TVS.

b. Krav for (CCI) kan være å nekte transaksjonsverifiseringstjenesten hvis hvilket som helst tvilling SIM eller viderekoblingsoppsettet for den aktuelle sluttbrukeren er oppdaget fra den integrerte telekom infrastrukturen.

c. Krav for (PI) kan nekte transaksjonsverifiseringstjenesten hvis korrelert geografisk avstand mellom web-IP av sluttbrukernes datamaskin og sluttbrukernes mobile posisjoneringsparameter er utenfor en akseptabel geografisk avstand oppgitt i VO.

(5) Det neste trinn av transaksjonsverifiseringsmekanismen starter en prosess hvor TVS omdanner det relevante innholdet som leveres i den mottatte VO til lydfiler med forskjellige formål.

a. Lydfil # 1 omfatter en syntetisk stemme som på det bestilte språket leser transaksjonsdetaljene.

b. Lydfil # 2 omfatter (PS) som en instrumentert lydmelding som skal bli streamet som en lydkrets gjennom lydbasert utstyr hos sluttbrukeren, Lydfilen # 2 er også utstyrt med feilretting og redundansmekanismer som sikrer høyere kvalitet og effektivitet av den etterfølgende lydoverføringen.

c. I tillegg kan det frembringes andre lydfiler med syntetisk tale, som genereres på basis av (II) for talebiometri,

(6) Det neste trinn i fremgangsmåten av transaksjonsverifiseringsmekanismen er at TVS forbereder seg på å sette opp anropet til brukeren på grunnlag av telefonnummeret som hentes fra VO.

a. I tilfelle (CCI) er bestilt, er TVS i stand til å oppdage tvilling-SIM, viderekoblingsoppsett, oppsett for telefonkonferanse eller andre relevante spørsmål fra telenettet avhengig av en sluttbrukeravtale med integrert teleoperatør,

b. I tilfelle (PI) er bestilt, er TVS i stand til å oppdage de geografiske posisjonsdata for hver av sluttbrukerenhetene -datamaskin og mobiltelefon, og om nødvendig i VO gir en korrelert avstand mellom enhetene,

c. I tilfelle (CCI) eller (PI) ikke oppfyller krav satt i VO, er en negativ kvittering til applikasjonsserveren tilgjengelig fra TVS som informerer om grunner for ikke å sette opp samtalen til sluttbruker.

(7) i tilfelle (CCI) og (PI) er oppfylt, setter TVS opp samtalen mot sluttbruker.

(8) Etter sluttbrukeren eventuelt har svart på anrop fra TVS, spiller TVS lydfilen # 1 over telefonsamtalepresentasjon av transaksjonsdetaljer i det bestilte språk, ved eventuelt å identifisere brukeren av en spesifisert metode hentet fra VO,

a. I tilfelle av en talebiometribasert metode for identifisering, med et tale biometrisk system integrert med TVS, er sluttbrukerens identitetsvalideringsoppgave gitt fra TVS til det integrerte talebiometri systemet som en sub-oppgave, venter på valideringsresultat før TVS fortsetter til neste fase av transaksjonsverifiseringsmekanismen.

b. Ved en annen biometrisk basert metode for identifisering ved hjelp av et biometrisk basert system integrert med TVS, er sluttbrukerens identitetsvalideringsoppgave gitt fra TVS til det integrerte biometrisystemet som en underliggende oppgave som venter på valideringsresultatet før TVS fortsetter til neste fase av transaksjonsverifiseringsmekanismen.

c. I tilfelle av en DTMF basert metode for identifisering, som krever av sluttbrukeren å taste inn en kode på telefonen, bruker DTMF lyder, med f.eks. et telefonbanksystem integrert med TVS, blir sluttbrukerens identitetsvalideringsoppgave gitt fra TVS til det integrerte systemet som en underliggende oppgave, som venter på valideringsresultat før TVS fortsetter til neste fase av transaksjonens verifiseringsmekanisme.

d. I tilfelle av en PKI-basert metode for identifisering, som krever sluttbrukeren til å bruke et bestemt sertifisertbasert system, integrert med TVS, blir sluttbrukerens identitetsvalideringsoppgave gitt fra TVS til det integrerte systemet som en underliggende oppgave, som venter på valideringsresultat før TVS fortsetter til neste fase av transaksjonens verifiseringsmekanisme.

(9) I tilfelle sluttbrukeren aksepterer transaksjonsdetaljer som presenteres mot brukeren over syntetisk tale fra lydfil # 1, blir brukeren bedt om å ta mikrofonen på telefonen mot høyttaleren av datamaskinen.

(10) Det neste trinnet er at TVS begynner å spille lydfilen # 2, som er streamet instrumentert lydmelding gjennom brukernes to enheter som bekrefter at utstyret er under både fysisk og logisk kontroll av den identifiserte brukeren. Ved å kontrollere fysisk bevegelse av telefonen, kan brukeren nå verifisere transaksjonen ved å la lydstrømmen fra høyttaleren på datamaskinen registreres av mikrofonen på telefonen.

a. Dersom brukeren ønsker å avbryte transaksjonsverifiseringen, må brukeren kun henge opp telefonsamtalen og dermed fysisk forby transaksjonen fra å bli utført.

(11) Dersom brukeren ønsker å godta transaksjonsverifiseringen ved at lydstrømmen blir fullt utført, blir innspilt lyd streamet senere bli levert som en innkommende audio stream over foreliggende telefonsamtale til TVS for dekoding. TVS vil etter dekoding sammenligne innkommende lyd med den utgående lyd av lydfil # 2.

a. Dersom inngående lyd sammenlignet med utgående lyd av lydfil # 2 er forskjellig, analyserer TVS bitstrømmen og lydpakkene, justerer innkommende lyd med feilretting og redundanstiltak av TVS lydbasert protokoll til perfekt match muligens er oppnådd.

b. Hvis perfekt match fortsatt ikke oppnås, analyserer TVS relevante pakker og starter sin adaptive retransmisjonsegenskaper av sin lydprotokoll for de aktuelle lydbaserte pakkene, før disse gjentakelsene av koding, retransmisjon, dekoding og sammenligning gir en perfekt match.

(L2) Hvis TVS-sammenligningen av innkommende og utgående (PS) innen en time-out innstilling får en perfekt match, en positiv kvittering med minimum innkommende dekodet (PS) og ordrenummeret blir sendt tilbake til applikasjonsserveren for behandling, applikasjonsserveren kan nå både sammenlikne (PS) sendt med (PS) mottatt og validere mottatt (PS) mot transaksjonshemmeligheten. Hvis denne valideringen gir et positivt resultat, vil applikasjonsserveren deretter godta transaksjonen.

a. Hvis TVS-sammenligningen av innkommende og utgående (PS) innen en time-out-innstilling aldri blir en perfekt sammenlikning, en negativ kvittering

med minimum innkommende dekodet (PS) og ordrenummeret blir sendt tilbake til applikasjonsserveren for behandling. Applikasjonsserveren vil da avvise transaksjonen.

5

Krav

1. Fremgangsmåte for å sikre en elektronisk transaksjon mellom en applikasjonsserver og en sluttbruker, hvori sluttbruker har tilgang til en telefon og en datamaskin med en høyttaler, applikasjonsserveren sender en verifikasjon til en transaksjonsverifikasjonsserver og er videre k a r a k t e r i s e r t v e d at:

- transaksjonsverifiseringsserveren konverterer verifikasjonen i minst to lydfiler,
- transaksjonsverifiseringsserveren setter opp en samtale til sluttbruker og spiller av den første lydfilen på telefonen til sluttbruker i henhold til parametere og transaksjonsopplysningen beskrevet i verifiseringsordren,
- hvis sluttbrukeren aksepterer transaksjonsdetaljene presentert som en syntetisk stemme i det aktuelle språket i løpet av telefonsamtalen, spiller transaksjonsverifiseringsserveren av den andre lydfilen som en utgående lyd-stream på sluttbrukerens datamaskinhøyttaler,
- den andre lydfilen registreres av mikrofonen på sluttbrukerne telefonen,
- den innspilte andre lydfilen blir overført fra mikrofonen på telefonen til transaksjonsverifikasjonsserveren via selve telefonsamtalen,
- transaksjonsverifiseringsserverens sammenlikner den utgående streamede andre lydfilen med den mottatte andre lydfilen, og
- om de samstemmer, sender transaksjonsverifikasjonsserveren en positiv kvittering til applikasjonsserveren,
- en negativ kvittering sendes til applikasjonsserveren i tilfelle sluttbruker ikke aksepterer transaksjonsdetaljene presentert av mekanismen ved å avslutte samtalen eller trykke på en knapp på telefonen, i tilfelle transaksjonsverifiseringsserveren ikke er i stand til å finne en likhet mellom utgående streamet lyd med den innkommende mottatte lyden, en negativ kvittering sendes til applikasjonsserveren.

2. Fremgangsmåte ifølge krav 1, hvori verifiseringsrekkefølgen omfatter minst et pålitelig telefonnummer, et ordrenummer, en proxy-hemmelighet, transaksjonsdetaljer og en språkindikator.

3. Fremgangsmåte ifølge krav 2, hvori verifikasjonsserver kan også inkludere en identifikasjonsindikator, en anropsstyreindikator eller en posisjonsindikator.

4. Fremgangsmåte ifølge krav 1, hvori den første audiofilen omfatter en syntetisk tale på det bestilte språket som leser transaksjonsdetaljene.

5. Fremgangsmåte ifølge krav 1, hvori den andre lydfilen omfatter proxy-hemmeligheten.