(12) **PATENT**

(19) NO (11) **332479** (13) **B1**

NORGE (51) Int Cl.
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04W 4/00 (2009.01)

Patentstyret

(21)	Søknadsnr	20090934	(86)	Int.inng.dag og søknadsnr
(22)	Inng.dag	2009.03.02	(85)	Videreføringsdag
(24)	Løpedag	2009.03.02	(30)	Prioritet
(41)	Alm.tilgj	2010.09.03		
(45)	Meddelt	2012.09.24		

(73) Innehaver EnCap AS, Gaustadalléen 21, 0349 OSLO, Norge
(72) Oppfinner Petter Taugbøl, Bestumveien 42 C, 0281 OSLO, Norge
Arne Riiber, Heimdalsgata 21, 0561 OSLO, Norge
(74) Fullmektig ip.coop (IPR SA), c/o Leogriff AS, Bygdøy Allé 4 , 0257 OSLO, Norge

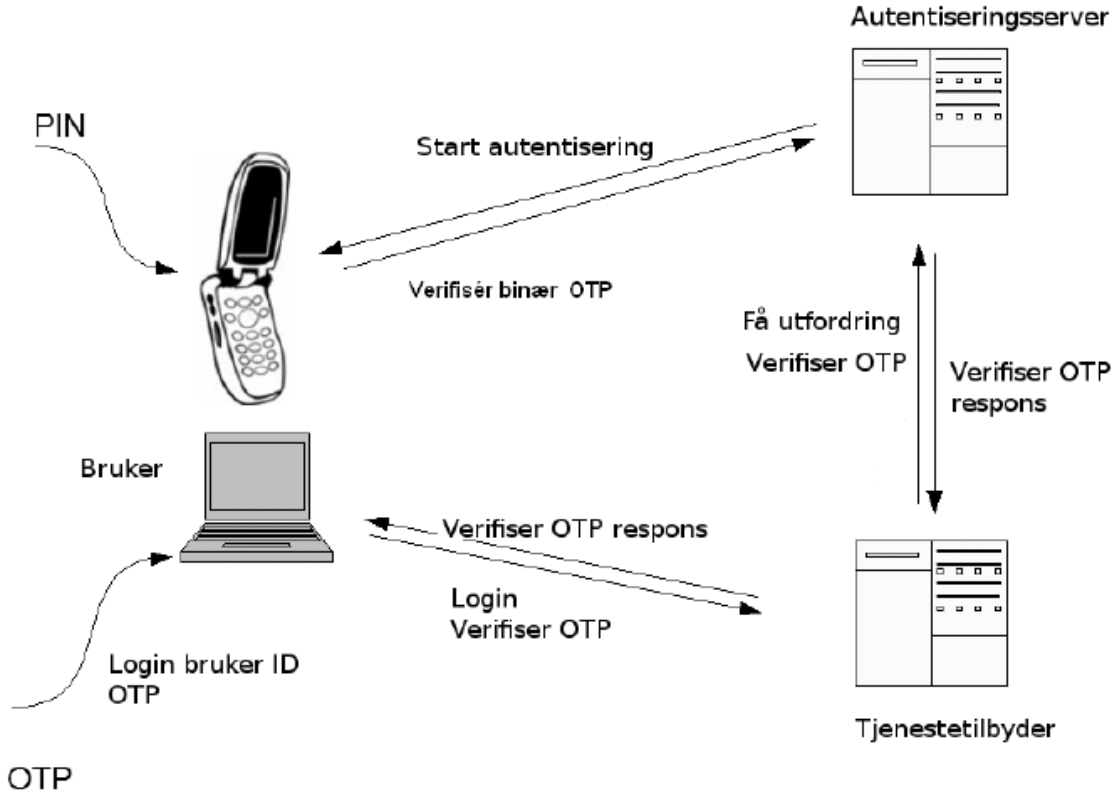
(54) Benevnelse **Fremgangsmåte og dataprogram for verifikasjon av engangspassord mellom tjener og mobil anordning med bruk av flere kanaler**

(56) Anførte publikasjoner

Using the mobile phone in two-factor authentication [Foredrag på IWSSI 2007 -First international Workshop on Security for spontaneousInteraction Program] Forfatter Anders Hagalisletto . Arne Riiber [lastet fra internett 2009.07.01] [Hentet fra http://www.comp.lancs.ac.uk/iwssi2007/][http://www.comp.lancs.ac.uk/iwssi2007/papers/iwssi2007-05.pdf]
WO 2009/009852 A2, WO 2007/145540 A2, KR 200080011938 A

(57) Sammendrag

En fremgangsmåte og dataprogram for generering og verifisering av engangspassord mellom to parter, en tjenesteyter og en bruker, hvor nevnte bruker har tilgang til minst to kommunikasjonskanaler og hvor nevnte bruker er logget på tjenestetilbyderen med en bruker ID via en kommunikasjonskanal og tjenestetilbyderen kan kommunisere med en autentiseringsserver som igjen kan kommunisere med brukeren via i det minste en annen kommunikasjonskanal enn tjenestetilbyderen.



Fremgangsmåte og dataprogram for verifikasjon av engangspassord mellom tjener og mobil anordning med bruk av flere kanaler.

Oppfinnelsens anvendelsesområde

Oppfinnelsen er innenfor feltet autentisering av brukere i elektroniske tjenester ved hjelp av OTP (engangs passord), og spesielt bruken av minst to kanaler for verifikasjon av engangspassord mellom tjener og mobil anordning.

Bakgrunn og tidligere kjent teknikk

Tilbydere av tjenester i elektroniske kanaler står ovenfor utfordringene med å autentisere brukerne av deres tjenester. Det å kunne tilby sikker autentisering av brukere er nødvendig for mange elektroniske tjenester.

Tjenestetilbydere som krever sterk brukerautentisering utsteder ofte en eller flere autentiseringsfaktorer til en bruker som tjenestetilbyder senere kan benytte for å autentisere brukeren. Hvis brukeren blir utstyrt med mer enn én autentisering faktor og brukeren må benytte alle autentiserings faktorene i en autentiseringssituasjon, så blir risikoen for feilaktige hendelser sterkt redusert. Hvis autentiseringsfaktorene i tillegg er av forskjellig natur, at hver gir en entydig identifikasjon av brukeren og at de autentiseringsdata som produseres er hemmelig for andre enn brukeren selv og tjenestetilbyderen, så blir løsningen det som i fagmiljøet kalles en sterk flerfaktor autentiserings løsning.

Autentiseringsfaktorer i vanlig bruk er: en kunnskapsfaktor('noe du vet', som et passord eller PIN kode) og en besittelsesfaktor ('noe du har', som en elektronisk engangspassord generator, en sikkerhets klient med private krypteringsnøkler lagret i et datamaskinminne eller på et smart-kort, trykte lister med engangs koder, skrapekort eller annet). I tillegg er noen ganger biometriske data ('noe du er', som digital representasjon av et fingeravtrykk eller iris skanning) brukt som en autentiseringsfaktor.

Besittelsesfaktorer er ofte av fysisk art, som smart-kort, passord kalkulatorer/dingser eller skrapekort. Det å utstede fysiske besittelsesfaktorer representerer ofte betydelige kostnader for tjenestetilbyderne og betraktes ofte som ubekvemme for brukerne. Det kan derfor være av interesse for tjenestetilbydere å benytte en generell, tilgjengelig brukerterminal som allerede er i brukerens hender, som en sikker besittelsesfaktor. Eksempler på personlige terminaler som det kan være attraktivt å benytte som besittelsesfaktor er utstyr med kommunikasjonsmuligheter slik som mobiltelefoner, bærbare datamaskiner, håndholdte datamaskiner som PDA-er og smart-telefoner og personlige underholdningsterminaler; for alle disse brukes uttrykket "mobil" her som en generisk betegnelse.

Mange fremgangsmåter for bruk av personlige dataterminaler til autentisering av brukere er kjent.

En fremgangsmåte er der en tjenestetilbyder registrerer brukernes mobil-abonnementsnummer og så i en autentiseringsprosess distribuerer en felles hemmelighet til brukerens mobilterminal, samtidig som det kreves at brukeren returnerer denne felles hemmeligheten i en annen

elektronisk kanal. Svakheten med denne fremgangsmåten er at senderen (tjenestetilbyder) ikke kan bekrefte identiteten til mottakende part (brukeren), den felles hemmeligheten er produsert på en tjener; og dermed er det ikke noen referanse til en besittelsesfaktor i autentiseringssvaret og mobilenheten er bare brukt som en kommunikasjonsterminal. Og egentlig er mobilterminalen ikke betraktet som et sikkert miljø for oppbevaring av felles hemmeligheter, - for eksempel kan felles hemmeligheter bli avslørt i nettverket eller lest av eller redistribuert til en annen part fra mobilterminalen, og derigjennom redusere den til en annen kunnskapsfaktor i stedet for en besittelsesfaktor – dvs det er nå to kunnskapsfaktorer (passord pluss passord sendt via sms) – noe som ikke er en ekte tofaktor løsning.

IETF RFC 4226 (http://www.ietf.org/rfc/rfc4226) fra Desember 2005 beskriver en algoritme for å generere engangspassord verdier, basert på Hashed Message Authentication Code, for bruk i tofaktor autentisering på Internet. Internet Utkast "OCRA: OATH Challenge-Response Algorithms draft-mraihi-mutual-oath-hotp-variants-08.txt" (http://tools.ietf.org/html/draft-mraihi-mutual-oath-hotp-variants-08) beskriver OATH algoritmen for challenge-response autentisering og signaturer. Denne algoritmen er basert på HOTP algoritmen i RFC4226.

IETF RFC 2289 (http://www.ietf.org/rfc/rfc2289) fra februar 1998 beskriver et One-Time Password System

WO/2006/075917 beskriver en fremgangsmåte for å produsere en sikkerhetskode ved hjelp av programmerbart brukerutstyr som kan benyttes til autentisering.

"Using the mobile phone in two-factor authentication" som ble presentert av Anders Hagalisletto og Arne Riiber

(http://www.comp.lancs.ac.uk/iwssi2007/papers/iwssi2007-05.pdf) viser hvordan man kan bruke en mobiltelefon til å vise et engangspassord.

KR20080011938A beskriver en metode hvor brukerens identitet blir autorisert av en tjener som sender en SMS med en modul for generering av engangspassord når det tastes inn en PIN. WO2009009852A2 beskriver en metode for å overføre tillit ved bruk av et mobilt utstyr for generering av engangspassord som fremvises basert på et personlig passord og koder.

WO2007/145540A beskriver tofaktor autentisering med en separat kanal mot autentiseringssystemet og bruk av et passord på mobilutstyret. Det er foreslått å bruke en trådløs kanal i tillegg, men med samme engangspassord.

DE10102779A1 beskriver et autorisasjonssystem for mobiltelefontransaksjoner som har separate koplinger til separate enheter i samme utstyr.

EP1919123A1 beskriver en tokanal challenge-response autentiseringsmetode der svaret sammenlignes med et underutvalg av autentiseringsbevis som er benyttet ved sesjonens autentiserings challenge.

I " Multi-channel protocols " av Ford-Lang Wong og Frank Stajano i B. Christianson et al. (Eds.): Security Protocols 2005, LNCS (http://www.cl.cam.ac.uk/~fms27/papers/2005-WongSta-multichannel.pdf)diskuteres bruken av flere kanaler. Bruk av et kamera og sending av bilder foreslås som en kanal.

Noen tilleggsproblemer med disse løsningene er:

* Sannsynligheten for vellykket autentisering av et falskt autentiseringsforsøk ved en tilfeldig OTP er større enn 1

delt på 10 opphøyet i E (antall siffer) for offline siffer baserte OTP enheter, noe som gjør det mulig å lage automatiske, distribuerte angrep som løper til vellykket autentisering av en tilfeldig OTP.

* Denial of Service (DOS) – tilgjengelighetsangrep kan igangsettes som låser OTP utstyret på tjenermaskinen, og dermed hindrer adgang selv for brukere med riktig OTP utstyr.

* Treg nettverkstilgang ved bruk av online mobile OTP enheter (et problem som er relevant ved online flerkanal OTP utstyr) – gjør at bruker må vente på klient/tjener kommunikasjonen før OTP kan vises. (Dette problemet eksisterer ikke ved bruk av off-line OTP utstyr.)

* MITM (Mann i Midten)angrep i en enkanal online autentiserings løsning, hvor OTP overføres gjennom en antatt sikker datakanal, for eksempel HTTPS.

Når flere kanaler brukes systematisk i et system for autentisering og verifikasjon, er det alltid en mulighet for at en kanal kan ha feil eller kommunikasjonsproblemer, eller at brukeren kan ha problemer med å fremskaffe informasjon i kanalen, for eksempel på grunn av et handikap. Det er da behov for en mer fleksibel behandling av verifikasjonsresultatet enn bare å konstatere at autentiseringen har feilet.

Sammendrag av oppfinnelsen

Oppfinnelsens gjenstand er en fremgangsmåte, arrangement og et dataprogram for bruk av en generelt tilgjengelig personlig dataterminal, en mobil, som en sikker og pålitelig besittelsesfaktor ved brukerautentisering.

Trekkene som beskrives i de vedlagte selvstendige kravene karakteriserer denne fremgangsmåten og arrangementet.

Oppfinnelsen inkluderer en lokal OTP generering med samtidig to-/flerkanal verifikasjon.

Kjent teknikk inkluderer:

- Offline OTP utstyr som har lokal OTP generering og enkanal bekreftelse.
- Online OTP utstyr som har klient/tjener kommunikasjon f.eks. for å motta en challenge (utfordring), og enkanal verifikasjon når utstyret viser OTP-kode til brukeren.

I en foretrukket versjon av denne oppfinnelsen taster brukeren PIN og dermed produseres en binær-OTP i klienten, denne binær-OTP-en konverteres til en lesbar skjerm-OTP på klienten slik at brukeren kan begynne å lese den og taste den i en annen kanal (kanal 2), samtidig med at binær-OTP-en overføres via mobilkanalen (kanal nr 1). Dette skjer simultant fordi mobilen overfører binær-OTP mens brukeren leser og taster skjerm-OTP på kanal nr 2. Skjerm-OTP er avledet fra binær-OTP. Binær-OTP er i et format som passer for datakommunikasjon og databehandling (f.eks. ren binær, eller kodet, f.eks. i hexadesimal notasjon eller base64, eller Unicode) og skjerm-OTP er egnet til å bli lest på en skjerm av et menneske og tastet inn på et tastatur, f.eks som bokstaver og tall vanligvis brukt av bruker eller tjeneste. Som vist i figurene 2, 3 og 4 blir binær-OTP generert i mobilutstyret, og det er også tilordningen til skjerm-OTP.

Følgende prinsipper gjelder:

- Tokanal verifikasjon av OTP.

- Lokal OTP generering, med simultan to- eller flerkanal verifikasjon og besvarelse av OTP verifikasjon på
  - mobil kanal(-er), f.eks.
    - SMS
    - Near Field Communications (NFC)
    - Wireless LAN (trådløs LAN)
    - Linje- eller pakkesvitsjede transmisjonsteknologier for mobilnett som CDMA, WCDMA, GSM, GPRS, 3G, 4G
    -
  - annen/andre kanaler, f.eks.
    a) en PC med en web kanal brukt til internett banktjenester,

    b) adgangskontroll på dører

    c) butikkterminaler

    d) minibanker

Brukeren trenger ikke å vente på verifikasjonen av binær-OTP. Brukeren kan starte å taste inn øyeblikkelig siden den lokale konverteringen fra binær-OTP til skjerm-OTP i praksis er mye raskere enn overføringstiden i mobilnettverket. Hvis brukeren taster feil PIN eller på annen måte forårsaker en feil binær-OTP, så får brukeren, etter at resultatet av verifikasjonen er ferdig på tjeneren, beskjed på begge kanaler om at autentiseringen har mislyktes.

Hvis binær-OTP er feil, vil verifikasjonen av binær-OTP mislykkes. Verifikasjon av skjerm-OTP vil også mislykkes fordi verifikasjonen av binær-OTP mislyktes.

Hvis en time-out oppstår i Autentiserings tjeneren fordi den ikke har mottatt binær-OTP, så kan verifikasjon av

skjerm-OTP mislykkes, siden verifikasjon av binær-OTP ikke har vært vellykket. Time-out kan være forårsaket av naturlige overføringsforsinkelser, eller forårsaket av en angriper.

Det er mulig å sette opp regler og parametre som kan tillate autentisering i spesielle situasjoner som et nettverksbrudd, dvs der det er kjent at en time-out er sannsynlig eller hvis det er kjent at en spesiell bruker har problemer med å taste inn skjerm-OTP, for eksempel på grunn av et handikap.

Det er også mulig å bruke f.eks. tekst-til-stemme og stemme gjenkjennings software eller å benytte "call center", for å gjøre det mulig for handikappede personer å bruke denne oppfinnelsen.

Med den foreliggende oppfinnelse er det mulig å hindre en type DOS- (tjenestenekt-) angrep for tjenester som benytter to-faktor autentisering. I en slik type DOS-angrep forsøker angriperen å sperre tjenesten ved å taste inn en vilkårlig feil OTP et antall ganger i web-kanalen, slik at OTP-enheten låses. Dette forhindres siden en kan se bort fra forsøk på verifikasjon av skjerm-OTP gjennom web-kanalen, hvis ikke binær-OTP gjennom mobil-kanalen har blitt verifisert vellykket.

Verifikasjonen av binær-OTP mellom mobilen og tjener øker sikkerheten knyttet til lengden av OTP, noe som oppfattes som et tilfeldig tall av en MITM (Mann I Midten), fordi en skjerm-OTP er typisk et 4-8 siffer tall som kan kodes som 2-4 bytes, mens binær-OTP-en er et tall på minst 16 bytes, lett utvidbart til 32 bytes eller mer. . Dermed er sannsynligheten for f.eks. gjennom prøving og feiling å finne eller gjette en binær-OTP mye mindre enn sannsynlighet for å finne en skjerm-OTP.

Grensesnitt som er kompatible med tradisjonelle challenge/response offline OTP løsninger kan brukes for å integrere et nytt flerkanal OTP verifikasjonsskjema i henhold til denne oppfinnelsen med en eksisterende enkanal løsning, for eksempel tids/sekvens basert offline OTP utstyr eller challenge-response skrapekort, noe som gjør det mulig å erstatte offline enkanal OTP verifikasjon mekanismer med herværende oppfinnelse.

Det er umulig for en MITM mellom Autentiserings klienten og Autentiserings tjeneren å observere skjerm-OTP på mobilkanalen, fordi denne OTP-en ikke blir overført på dét grensesnittet. Skjerm-OTP-en blir generert av Autentiserings klienten og vises for brukeren, basert på binær-OTP og PIN (Personal Identification Number).

Bruken av PIN kan være en opsjon. Bruken av PIN vil da typisk være tilrettelagt gjennom en konfigurerbar parameter per system eller per enhet. Hvis PIN ikke brukes, er tilordningen mellom binær-OTP og skjerm-OTP enten samme algoritme uten PIN eller en spesiell algoritme for den spesielle klienten, kjent for autentiseringstjeneren, for bruk uten PIN.

Kort beskrivelse av tegninger

Figur 1 gir et eksempel på komponentene involvert i en tokanal verifikasjonssekvens i en versjon bestående av en mobiltelefon og en datamaskin.

Figur 2 viser detaljert autentiseringssekvens med tokanals parallell OTP verifikasjon.

Figur 3 viser en sekvens med bruker challenge.

Figur 4 viser en sekvens uten bruker challenge.

Figur 5 viser en alternativ metode for å generere skjerm-OTP og binær-OTP i autentiseringstjeneren.

Figur 6 viser den foretrukne metoden for å generere skjerm-OTP og binær-OTP i autentiseringstjeneren.

Figur 7 viser kildekode fra en foretrukket løsning for konvertering av binær-OTP til skjerm-OTP.

Detaljert beskrivelse

Figur 1 viser et eksempel på en realisering av denne oppfinnelsen. Den gir en oversikt over de forskjellige komponenter som er involvert i oppfinnelsen. I denne figuren vises det hvordan en bruker kobler til og logger seg inn hos en tjenestetilbyder.

Når brukeren skal gjennomføre en transaksjon kobler tjenestetilbyderen seg til autentiseringstjeneren som igjen starter en autentisering via brukerens mobil som har installert den spesielle softwaren fra Autentiserings autoriteten. Denne softwaren kan være implementert på mange måter f.eks. avhengig av mobilens operativsystem. En foretrukket realisering av softwaren er implementert basert på Java for mobilterminaler (MIDP2/J2ME) fra Sun. Tjeneren er i den foretrukne realiseringen basert Java enterprise serverplattform (J2EE).

Når autentiseringstjeneren starter autentiseringsprosessen skal brukeren taste PIN på mobilen, softwaren i telefonen generer en OTP (skjerm-OTP) og en binær-OTP, binær-OTP-en blir sendt til autentiseringstjeneren og brukeren må taste inn den tilhørende OTP (skjerm-OTP) i applikasjonen som

kommuniserer med tjenestetilbyderen, vanligvis en web-side. Tjenestetilbyderen sender skjerm-OTP til autentiseringstjeneren som verifiserer skjerm-OTP-en. Autentiseringstjeneren verifiserer også binær-OTP-en som ble mottatt fra mobilen. Autentiseringstjeneren genererer resultatet av de to verifisér OTP operasjonene i henhold til regler og parametere, og sender svaret til tjenestetilbyderen som igjen sender verifikasjonssvaret til brukeren, vanligvis via web kanalen ved hjelp av den resulterende web siden, og sender også svaret til mobilen via mobilkanalen, normalt til skjermen på mobilen, skjønt det kan også suppleres med eller erstattes av for eksempel lyd eller følbar tilbakemelding.

Hvis autentiseringen er initiert av en push-melding, kan autentiseringstjeneren sende challenge (utfordringen) til autentiseringsklienten i den samme meldingen. I en alternativ realisering blir challenge sendt i mer enn én kanal.

Det vises hvordan autentisering og kommunikasjon skjer via to forskjellige kommunikasjons kanaler, noe som gjør det vanskelig for en fremmed part å bryte inn i kommunikasjonen fordi vedkommende da må snappe opp kommunikasjonen på to forskjellige typer kommunikasjonsforbindelser. Den eneste muligheten en fremmed part har til å blande seg inn i transaksjonen, er at han har mulighet til å bryte inn i begge kommunikasjonssesjoner eller at de har stjålet både brukerens datamaskin og mobiltelefon og kjenner PIN koden og innloggingsinformasjonen. Begge disse scenariene er vanskelige å gjennomføre.

Figur 2 er en detaljert beskrivelse av autentiseringssekvensen i et challenge/response scenario.

Brukeren taster brukerID på web innloggings siden og sender siden til Tjenestetilbyder.

Bruker ID kan være en hvilken som helst bruker spesifikk informasjon som en PIN-kode, et telefonnummer, personnummer, et selvvalgt eller systemgenerert ID, en kode eller til og med biometrisk input. Bruker ID er unik for den enkelte bruker. En bruker må ikke nødvendigvis være én enkelt person, men bruker ID kan også være brukt av en gruppe personer, men i den foretrukne realiseringen vil Bruker ID entydig identifisere én person.

Tjenestetilbydere slår opp mobiltelefonnummeret (msisdn) til brukeren og sender en forespørsel om en ”challenge” (et tilfeldig tall) til Autentiseringstjeneren. Challenge blir sendt via web siden (eller i kode via web siden) til Brukeren. Challenge inneholder eller initierer tekst som instruerer Brukeren om å taste inn OTP-en fra en annen applikasjon som også ligger på mobilen. En challenge ID assosiert med innloggingsforsøket blir også returnert i web siden (eller i kode gjennom web siden) til Brukeren, dette tillater flere utestående ikke-fullførte innlogginger i en challenge/response løsning, men flerkanal verifikasjon fungerer også uten slik challenge ID.

Autentiseringstjeneren sender en push start autentiserings melding til Autentiseringsklienten på brukerens mobil. Autentiseringstjeneren kjenner noe i Autentiserings klienten som kan brukes til å generere OTP. I den foretrukne løsningen gjøres dette som beskrevet i WO/2006/075917 og ved bruk av challenge.

Autentiseringsklienten ber om en challenge fra Autentiseringstjeneren, hvis denne ikke var inkludert i den initiale meldingen, og ber brukeren om å taste PIN.

Autentiseringsklienten generer binær-OTP, konverterer den til en menneskelig lesbar skjerm-OTP, viser denne, og starter overføring av binær-OTP til Autentiserings-tjeneren. Forsinkelse i overføringen som er vanlig i en typisk mobilkanal med liten båndbredde, er antydet i figuren gjennom å utsette meldingen "verifisér binær-OTP" til etter at web-leseren har sendt OTP (skjerm-OTP).

Brukeren taster skjerm-OTP i web-leseren og sender den til Autentiseringstjeneren via Tjenestetilbyderen.

Autentiseringstjeneren venter i en konfigurerbar tidsperiode inntil binær-OTP blir verifisert, eller har gått ut på tid .

Autentiseringstjeneren mottar "verifisér binær OTP" meldingen, verifiserer binær- og skjerm-OTP, og returnerer resultatet i begge kanaler.

Figur 3 illustrerer autentiseringssekvensen for en OTP enhet der brukeren mottar challenge fra web siden, starter klienten,og taster challenge inn i klienten.

Figur 4 illustrerer autentiseringssekvensen for en OTP enhet uten challenge. Brukeren starter klienten manuelt.

Figur 5 illustrerer en fremgangsmåte for å generere skjerm-OTP og binær-OTP i autentiseringstjeneren. En tilsvarende prosess finner sted i autentiseringsklienten. I denne løsningen genereres skjerm-OTP og binær-OTP ved hjelp av forskjellige algoritmer og kunne også ha vært basert på to sett av data som var lagret sammen med brukerprofilen. En algoritme som kunne ha vært brukt er en oppslagstabell som beskrevet i [RFC2289].

Figur 6 viser den foretrukne fremgangsmåten for generering av skjerm-OTP og binær-OTP i autentiseringstjeneren. En

tilsvarende prosess finner sted i autentiseringsklienten. Skjerm-OTP blir utledet ved å benytte binær-OTP kombinert med en algoritme. I denne foretrukne løsningen er følgende algoritmer benyttet:

- for generererering av binær-OTP: challenge response som vist i by WO/2006/075917
- for generering av skjerm-OTP: GenerateOTP() metoden fra RFC4226, med:
    - binær-OTP som nøkkel (i stedet for HMAC-SHA1 som er beskrevet i RFC4226) , og
    - challenge som movingFactor, og
    - konfigurerbart antall siffer som skal vises

Figur 7 illustrerer dette med kildekode for dette steget i den foretrukne løsningen. Her er binær-OTP 16 byte og skjerm-OTP er 6 siffer, normalt/tilsvarende 3 byte. Dette sikrer en brukervennlig skjerm-OTP og en lengre, sterkere binær-OTP.

Near Field Communication (NFC) er en kortholds høy-frekvent trådløs kommunikasjonsteknologi som tillater utveksling av data mellom utstyr på opp til 10 centimeters avstand, som dermed har mye kortere rekkevidde enn for eksempel Bluetooth (Blåtann) eller andre kortholds radiokommunikasjonforbindelser. NFC er tilgjengelig i mobiltelefoner som Nokia 3220 og i nyere modeller fra denne og andre leverandører. NFC er velegnet for autentiseringsformål som en besittelsesfaktor som må holdes svært nær til den andre enheten og radiokanalen er dermed vanskelig å koble seg inn på.

I en annen realisering blir binær-OTP som genereres på mobilutstyret overført til en tjenestetilbyder gjennom bruk av NFC.

I nok en annen realisering blir binær-OTP som genereres på mobilen overført til en tjenestetilbyder ved bruk av en kortholds radiooverføringsforbindelse som Bluetooth.

I nok en annen realisering er OTP utstyret og besittelsesfaktoren med autentiseringsklienten i form av dataminne, for eksempel på et smartkort knyttet til mobiltelefonen eller PC (vertsutstyr) som har skjermen, behandlingsenheten og kommunikasjonskanalene som er nødvendige. Kortet kan for eksempel være en Subscriber Identity Module (SIM), et USB masselagringskort eller et SD kort. I denne løsningen må vertsutstyret skille mellom de to kommunikasjonskanalene.

Patentkrav

1. En fremgangsmåte for flerkanalsverifikasjon av engangs passord(OTP) mellom to parter bestående av en tjenestetilbyder og en bruker, hvor nevnte bruker har tilgang til minst to kommunikasjonskanaler, og hvor nevnte bruker logger på mot nevnte tjenestetilbyder med en brukerID via én kommunikasjonskanal, og nevnte tjenestetilbyder har mulighet til å kommunisere med en autentiserings tjener som igjen har mulighet til å kommunisere med nevnte bruker via minst én annen kommunikasjonskanal enn tjenestetilbyder, og hvor nevnte fremgangsmåte videre er karakterisert ved at:

- en autentiseringsklient genererer minst to forskjellige engangspassord, det første med lengde typisk over 16 bytes beregnet på behandling i maskiner, benevnt binær-OTP, og et andre avledet av det første på en form beregnet på å oppfattes av mennesker med lengde typisk 2-4 bytes, benevnt skjerm-OTP,

- nevnte autentiseringsklient overfører binær-OTP til nevnte autentiseringstjener ved bruk av en første kommunikasjonskanal,

- nevnte bruker taster skjerm-OTP som sendes i en andre kommunikasjonskanal og sender det til nevnte autentiserings tjener gjennom nevnte tjenestetilbyder.

- Når binær-OTP og skjerm-OTP er mottatt av autentiseringstjeneren blir de gjenstand for verifikasjon.

2. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 1, karakterisert ved at nevnte autentiserings klient ber om en utfordring fra nevnte autentiserings tjener og ber nevnte bruker å taste PIN.

3. En fremgangsmåte for flerkanalsverifikasjon av engangspassord (OTP) i følge krav 1, karakterisert ved at nevnte autentiseringstjener mottar binær-OTP meldingen, verifiserer binær og/eller skjerm-OTP, og returnerer resultatet i minst én kanal.

4. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 2, karakterisert ved at genereringen av engangspassord bli gjort både med eller uten PIN og med eller uten utfordring (challenge)

5. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 1, karakterisert ved at minst én kommunikasjonskanal bruker et mobilutstyr.

6. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 1, karakterisert ved at nevnte bruker logger på mot tjenestetilbyder via en nettleser.

7. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 1, karakterisert ved at nevnte bruker taster bruker ID i innloggingssiden på web og sender siden til Tjenestetilbyder.

8. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 4, karakterisert ved at nevnte utfordring (challenge) blir returnert i web-siden.

9. En fremgangsmåte for flerkanalsverifikasjon av engangpassord ifølge krav 4, karakterisert ved at nevnte utfordring (challenge) inneholder eller initierer tekst som instruerer Brukeren om å taste OTP fra en annen applikasjon som finnes på mobilen.

10. En fremgangsmåte for flerkanalsverifikasjon av engangspassord ifølge krav 4, karakterisert ved at nevnte utfordringsID (challenge ID) assosiert med innloggingsforsøket også blir returnert i web-siden.

11. En fremgangsmåte for flerkanals verifikasjon av engangspassord ifølge krav 4, karakterisert ved at nevnte utfordring (challenge) er inneholdt i en start push autentiseringsmelding til autentiseringsklienten på brukerens mobil.

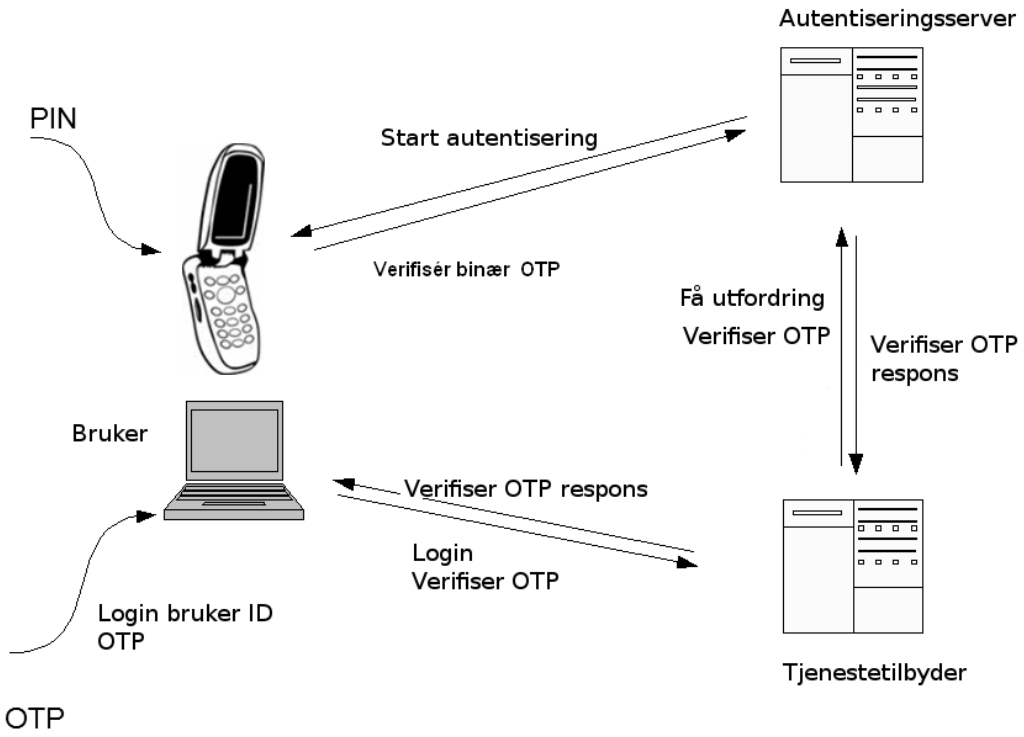
12. En fremgangsmåte for flerkanals verifikasjon av engangspassord ifølge krav 1, karakterisert ved at nevnte binær-OTP generert på nevnte mobilutstyr blir overført både til autentiseringstjeneren via én kommunikasjonskanal og til tjenestetilbyder via den andre kommunikasjonskanalen.

13. En fremgangsmåte for flerkanals verifikasjon av engangspassord ifølge krav 1, karakterisert ved at én kommunikasjonskanal benytter Near Field Communication eller kortholds radiooverføring.

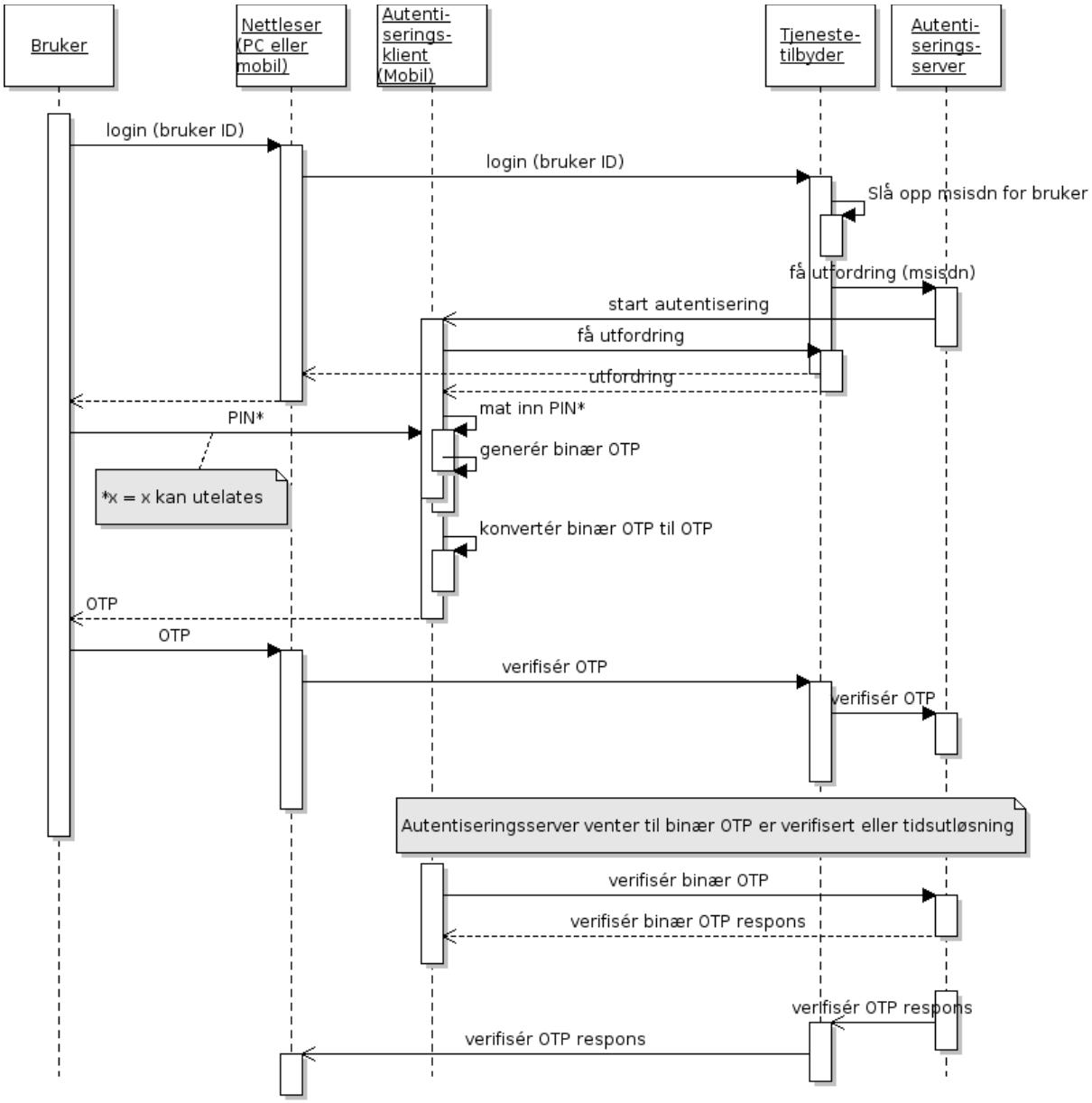
14. Dataprogram som kan lastes inn i internminnet i en behandlingsenhet i et datamaskinbasert system, omfattende programkodedeler for utføring av autentiseringen av nevnte bruker ifølge hvilke som helst av kravene 1 til 13.

15. Dataprogramprodukt lagret på et datamaskinlesbart medium, omfattende et lesbart program som forårsaker at behandlingsenheten i et datamaskinsystem kontrollerer en utførelse av autentisering av nevnte bruker ifølge hvilke som helst av kravene 1 til 13.

FIGURER

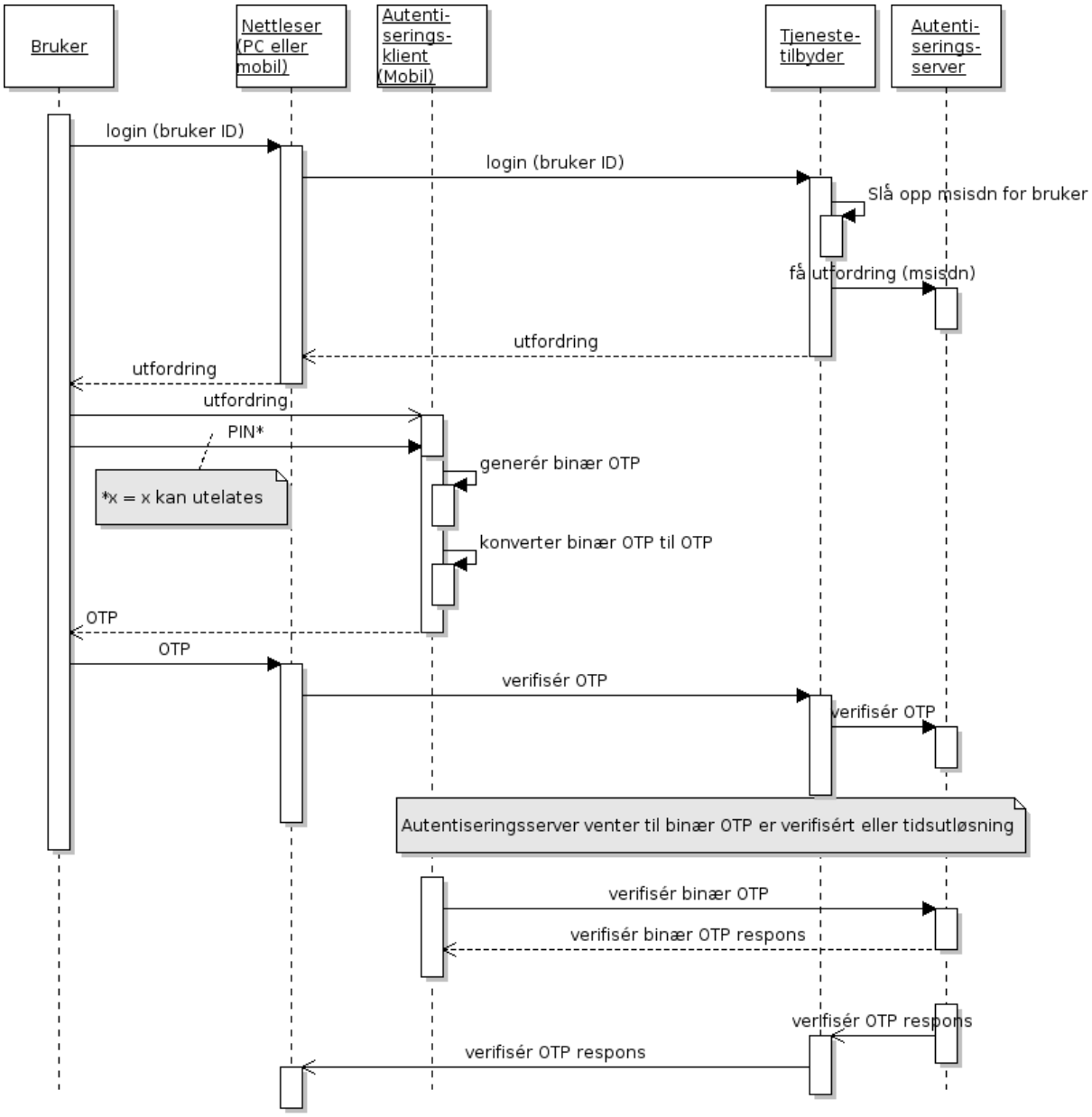


Figur 1


Bruker
Nettleser (PC eller mobil)
Autenti-serings-klient (Mobil)
Tjeneste-tilbyder
Autenti-serings-server
login (bruker ID)
login (bruker ID)
Slå opp msisdn for bruker
få utfordring (msisdn)
start autentisering
få utfordring
utfordring
mat inn PIN*
PIN*
generér binær OTP
*x = x kan utelates
konvertér binær OTP til OTP
OTP
OTP
verifisér OTP
verifisér OTP
Autentiseringsserver venter til binær OTP er verifisert eller tidsutløsning
verifisér binær OTP
verifisér binær OTP respons
verifisér OTP respons
verifisér OTP respons

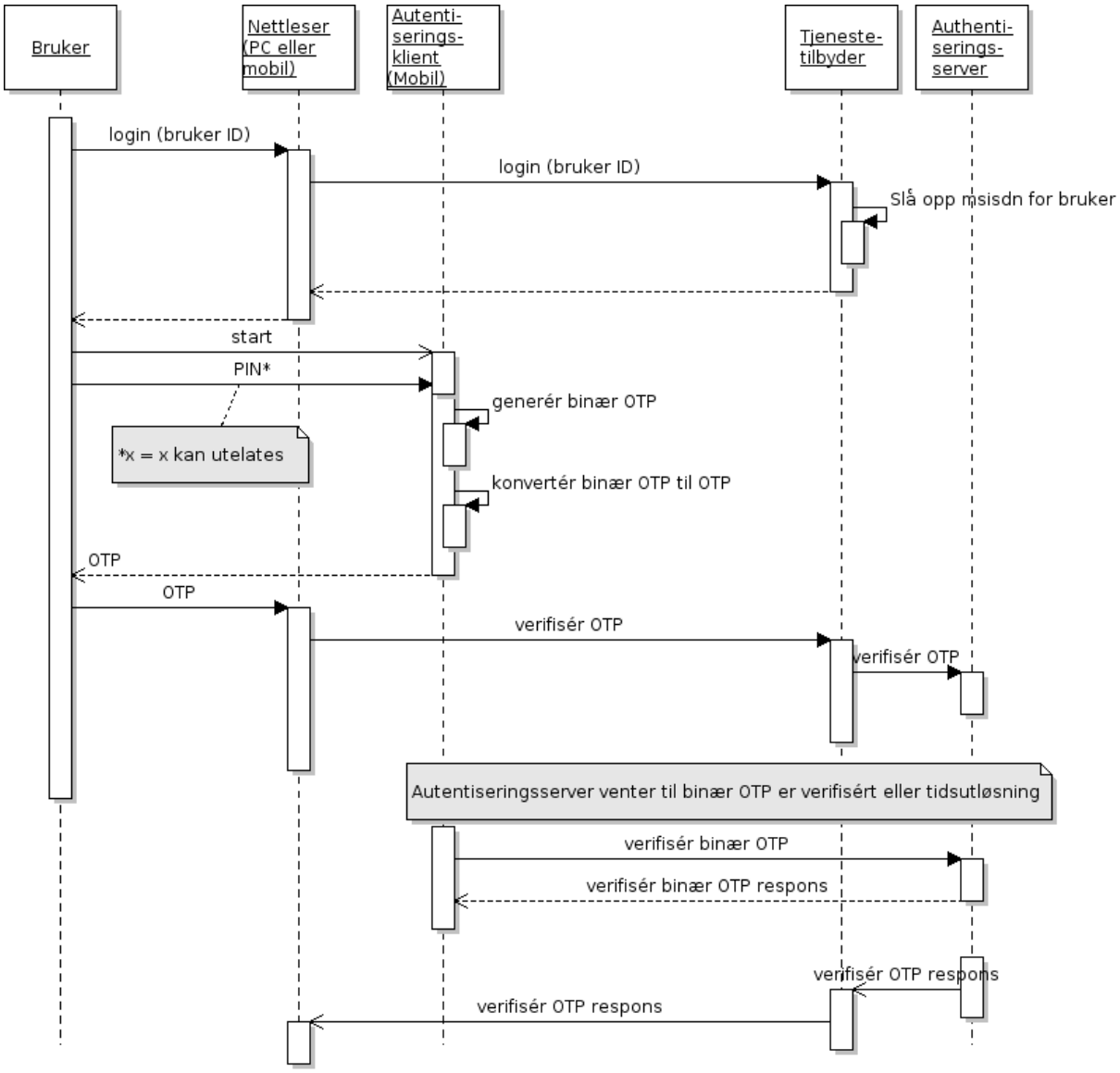
Figur 2

5

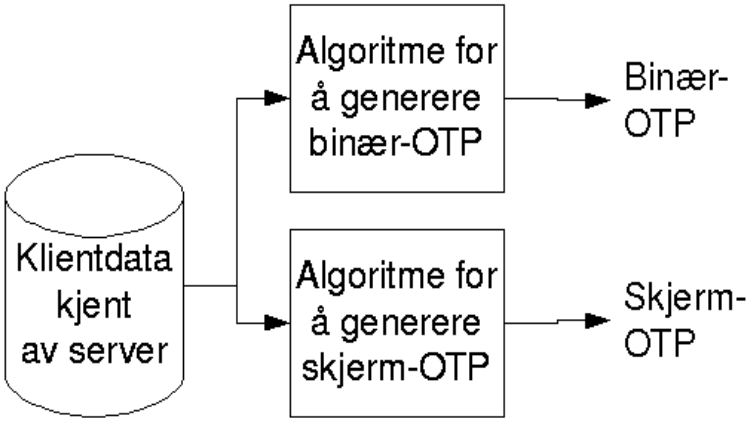

Bruker
Nettleser (PC eller mobil)
Autenti-serings-klient (Mobil)
Tjeneste-tilbyder
Autenti-serings-server
login (bruker ID)
login (bruker ID)
Slå opp msisdn for bruker
få utfordring (msisdn)
utfordring
utfordring
utfordring
PIN*
*x = x kan utelates
generér binær OTP
konverter binær OTP til OTP
OTP
OTP
verifisér OTP
verifisér OTP
Autentiseringsserver venter til binær OTP er verifisért eller tidsutløsning
verifisér binær OTP
verifisér binær OTP respons
verifisér OTP respons
verifisér OTP respons

Figur 3

5

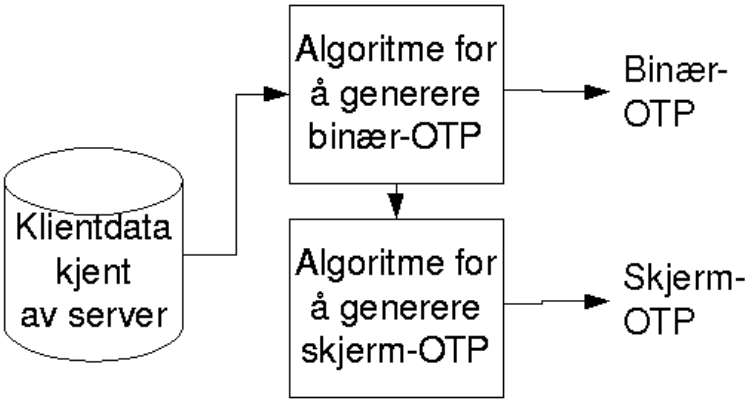

Bruker
Nettleser (PC eller mobil)
Autenti-serings-klient (Mobil)
Tjeneste-tilbyder
Authenti-serings-server
login (bruker ID)
login (bruker ID)
Slå opp msisdn for bruker
start
PIN*
*x = x kan utelates
generér binær OTP
konvertér binær OTP til OTP
OTP
OTP
verifisér OTP
verifisér OTP
Autentiseringsserver venter til binær OTP er verifisért eller tidsutløsning
verifisér binær OTP
verifisér binær OTP respons
verifisér OTP respons
verifisér OTP respons

Figur 4



Skjerm-OTP er uavhengig av binær-OTP

Figur 5



Skjerm-OTP er avledet av binær-OTP

Figur 6

```
/**
* Konvertér binær OTP til en OTP som kan bli fremvist
* Ifølge RFC4226 men med en utfordring (challenge) som bevegelig faktor
*
* RFC4226: HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))
* hvor K er den hemmelige nøkkelen og  C er telleren
*
* Vi tar binær OTP som den hemmelige nøkkelen, og utfordringen (challenge)
 * som telleren. En annen mulighet kan være å bruke sikkerhetskoden som den
hemmelige nøkkelen.
*/
private String toDisplayOtp(byte[ ] binaryOtp, byte[ ] challenge, int nDigits) {
      byte[ ] key = binaryOtp;
      // ensure correct length of movingFactor
      byte[ ] movingFactor = new byte[8];
      System.arraycopy(challenge, 0, movingFactor, 0, movingFactor.length);
      String displayOtp = null;
      try {
         displayOtp = OneTimePasswordAlgorithm.generateOTP(key,
movingFactor, nDigits, -1);
```

Figur 7