NORGE

(12) **PATENT**

(19) NO (11) **314649** (13) B1

(51) Int Cl[7] H 04 L 9/32

Patentstyret

(21) Søknadsnr	20012029	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	2001.04.25		
(24) Løpedag	2001.04.25	(85) Videreføringsdag	
(41) Alm. tilgj.	2002.10.28	(30) Prioritet	Ingen
(45) Meddelt dato	2003.04.22		

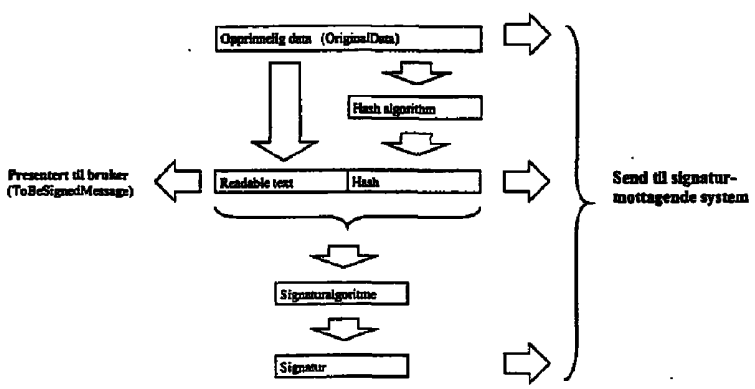
(71) Patenthaver Telefonaktiebolaget L M Ericsson, S-126 25 Stockholm, SE
(72) Oppfinner Sverre Tønnesland, 0659 Oslo, NO
Pål Bjølseth, 0276 Oslo, NO
(74) Fullmektig Oslo Patentkontor AS, 0306 Oslo

(54) Benevnelse **Fremgangsmåte for ikke-repudiering ved bruk av kryptografiske signaturer i små enheter**

(56) Anførte publikasjoner
WO 9905819
WML-Script Crypto Library fra http://www.wapforum.org spesielt kapittel 6
WO 0039958

(57) Sammendrag

En fremgangsmåte for å tilveiebringe elektronisk signering av data ved å benytte begrensede signeringsanordninger er angitt. Dette oppnås ved å trekke ut en del av dataene i et signaturbenyttende system, å kompilere det til en ren protokoll som benyttes av signeringsanordningen og å overføre det til nevnte signeringsanordning sammen med en hash av dataene. Brukeren av signeringsanordningen vil da bli presentert for den kompilerte del av dataene som er tilpasset i henhold til begrensningene i signeringsanordningen og som er forståelig for brukeren. Brukeren kan da elektronisk signere dataene ved hjelp av signeringsanordningen ved å benytte en passende signaturalgoritme. En riktig hash beviser at brukeren faktisk signerer de opprinnelige data, selv om han/hun bare blir presentert for en forståelig og signeringsanordningstilpasset del av dataene. Den resulterende signatur returneres til det signaturbenyttende system, og original data, delen av dataene, og hashen og signaturen sendes til et signaturmottagende system for prosessering, verifisering, lagring ete.



Figur 2 Konstruering av melding som skal sendes til det signaturmottagende system

Oppfinnelsens område

Den foreliggende oppfinnelse vedrører sammenkoblede dataanordninger, spesielt når kryptografisk signering benyttes for å oppnå kompabilitet (non-repudiation), aksesskontroll, brukerverifisering etc.

Oppfinnelsens bakgrunn

Mange type applikasjoner, for eksempel e-commerce eller m-commerce, krever muligheten til å skaffe til veie varig bevis på at noen har autorisert en transaksjon. Det forventes også at signering av elektronisk materiale, slik som avtaler, forretningsrapporter og forskjellige typer skjemaer blir vanlig i nær fremtid.

E-commerce og m-commerce er stadig voksende forretningsområder, og både offentlige og private administrasjoner ser nå ut til å gjøre de tilpasninger som skal til for å åpne for elektronisk signering. Et gjennombrudd for elektronisk signering er imidlertid avhengig av sikre, motstandsdyktige og enkle prosedyrer og løsninger. Den signerende part må være sikker på at det han/hun signerer er det samme som mottas hos den mottagende part. Den mottagende part må være sikker på at den signerende part er den hun/han utgir seg for å være. Videre bør signeringen være enkel uten at det kreves noen teknisk kunnskap fra brukeren, og bør fortrinnsvis være mulig å gjennomføre uavhengig av tid og sted.

Kryptografiske signaturer blir benyttet på en rekke områder. Dette involverer typisk i tillegg til brukeren, være seg eieren av den kryptografiske signeringsanordning, et signaturbenyttende system og et signaturmottagende system. Det signaturbenyttende system spør brukeren om å legge på en kryptografisk signatur på dataene som presenteres. Brukeren signerer og returnerer signaturen tilbake til det signaturbenyttende system. Det signaturbenyttende system kan overføre dataene som ble signert og signaturen til det

signaturmottagende system. Det signaturmottagende system er en kryptografisk bindingsrelasjon mellom hva det signaturbenyttende system presenterte til brukeren for signering og hva brukeren faktisk signerte.

PKI (Public Key Infrastructure) er et mye benyttet system for krypterisk signering og autentifisering, som er velkjent for fagfolk på området. En betrodd part i et PKI-system utsteder elektroniske nøkkelpar. Paret består av en privat nøkkel og en offentlig nøkkel. Den private nøkkelen er bare kjent for brukeren (eller brukerens signeringsanordning), men den offentlige nøkkel kan være kjent for en hvilken som helst annen part som skal motta signert data fra en bruker. I brukerens anordning er objektet som skal signeres og den private nøkkel input til en eller annen algoritme som gir ut objektet i signert tilstand. Ved den mottagende part er det signerte objekt og den offentlige nøkkel input til en annen algoritme som trekker ut det opprinnelige objektet fra det signerte objektet. Objektet vil bli trukket ut riktig kun hvis det var den korresponderende private nøkkelen som signerte det. Følgelig kan den mottagende part være sikker på at objektet ble signert av den bestemte bruker når denne brukers offentlige nøkkel benyttes for å trekke ut det opprinnelige objekt fra det signerte objekt.

Mange elektroniske anordninger støtter allerede kryptografisk signering. Et eksempel er en PC med en internettbrowser installert. Browseren kan ha en eller flere sertifikater som inneholder offentlige nøkler utstedt fra en eller flere betrodde parter eller såkalte sertifikatautoriteter (CA).

Et problem med dette er at en PC vanligvis er bundet til en fast plassering og/eller er for stor til å kunne bli båret rundt overalt. Behovet for å signere materiale er imidlertid ikke begrenset til steder hvor PC-er er plassert eller kan medbringes.

Videre er en PC som er on-line til enhver tid eller for lengre perioder svært sårbar for dataspionering, og det kan være en risiko for at inntrengere får tak i de private nøklene. Av sikkerhetshensyn kan bruker komme til å ønske å benytte hans/hennes personlige signeringsanordning for å signere materiale presentert på PC-en.

Løsningen på de ovenfor nevnte problemer kan være små portable anordninger slik som mobiltelefoner. "WMLScript Language Specification", WAP Forum, beskriver en implementering av en funksjon som gjør det mulig for WAP-telefoner å gjennomføre kryptografisk signering. WAP-telefonen spør brukeren om å signere en tekststreng ved å taste inn for eksempel en PIN-kode i anordningen for kryptografisk signering av strengen.

Slike anordninger, for eksempel mobiltelefoner, er imidlertid karakterisert ved at de er minne- og prosesseringskapasitetsbegrenset, og den kryptografiske signeringsfunksjonen er tilgjengelig gjennom et definert og begrenset grensesnitt.

Videre har små anordninger som mobiltelefoner normalt ikke en grafisk skjerm eller store programmer som PowerPoint og Word installert.

Problemene oppstår da når dataene som skal signeres er for store til å bli presentert til brukeren, eller er i et format som ikke er forståelig for brukeren eller som ikke er kompatible for signeringsanordningen. Den ovenfor nevnte spesifikasjon forutsetter imidlertid at dataene er forståelige og små nok til å kunne bli presentert på hardware og skjermbegrensede anordninger.

Oppsummering av oppfinnelsen

Hovedformålet med den foreliggende oppfinnelse er å overvinne de ovenfor nevnte problemer og tilveiebringe kompabi-

litet mellom en bruker, et signaturbenyttende system og et signaturmottagende system. Dette oppnås gjennom en fremgangsmåte definert av det vedlagte krav 1.

Nærmere bestemt tilveiebringer den foreliggende oppfinnelse en fremgangsmåte for digital signering av data ved å benytte en signeringsanordning ved å trekke ut en del av dataene i et signaturbenyttende system, kompilere det til en brukbar protokoll som benyttes av signeringsanordningen og overføre den til nevnte signeringsanordning sammen med en hash-kode av dataene. Brukeren av signeringsanordningen vil da bli presentert for den kompilerte del av dataene, som er tilpasset i henhold til signeringsanordningens begrensninger og er forståelig for brukeren. Brukeren kan da elektronisk signere dataene ved hjelp av signeringsanordningen ved å benytte en passende signaturalgoritme. En riktig hash-kode beviser at brukeren faktisk signerte de riktige dataene, selv om han ble presentert kun for den forståelige og justerte delen av dataene. Den resulterende signatur returneres til det signaturbenyttende system, og de opprinnelige data, delen av dataene, hash-koden og signaturen sendes til et signaturmottagende system for prosessering, verifisering, lagring etc.

Den foreliggende oppfinnelse gjør det mulig å benytte hardware og prosessorbegrensede signeringsanordninger, for eksempel mobiltelefoner, for å signere data som er for store for signeringsanordningen.

Kort beskrivelse av tegningene

Figur 1 illustrerer problemet med å signere ikke-lesbar tekst på en liten anordning.

Figur 2 er et flytskjema som viser dataflyten i en utførelse i henhold til den foreliggende oppfinnelse.

Figur 3 viser hvordan dataene kan overføres mellom elementene som er involvert i en utførelse i henhold til den foreliggende oppfinnelse.

Figur 4 viser et eksempel på dataflyten i en "push"-signeringsforespørsel som benytter en WAP 1.2 mobilanordning hvor HTTP benyttes mellom et signaturbenyttende og et signaturmottagende system.

Figur 5 er et bilde over hvordan en uttrukket tekst fra et opprinnelig objekt som skal signeres kan se ut.

Foretrukne utførelser av den foreliggende oppfinnelse

I det følgende beskrives en foretrukket utførelse av den foreliggende oppfinnelse. Legg merke til at denne utførelsen diskuteres kun av illustrasjonshensyn, og begrenser ikke oppfinnelsen slik den er definert i det vedlagte krav 1.

Utførelsen som er beskrevet, tilveiebringer en fleksibel måte å implementere den kryptografiske binding mellom en bruker og et datasett som er uforståelig for mennesker i dets opprinnelige form, eller for stort til å kunne bli presentert for brukeren for signering. Den er delvis beskrevet i en protokollsyntaks med referanse til de ovenfor nevnte tegninger.

Figur 3 illustrerer et "push"-scenario, hvor det signaturbenyttende system kobler seg opp til den lille kryptografiske anordning og sender over signaturforespørselen. I et "pull"-scenario kobler den lille kryptografiske anordning seg til det signaturbenyttende system og spør etter dataene som skal signeres.

Det signaturbenyttende system og det signaturmottagende system er logiske entiteter i et databehandlingsnett. De kan befinne seg i samme nettkomponent eller de kan være separa-

parate fra hverandre som i eksemplifiseringen ovenfor, hvor det signaturbenyttende system er brukerens PC.

Det signaturbenyttende system kompilerer (2) en sammenstilt (1) melding på en slik måte at den kan presenteres og forstås av brukeren. Det signaturbenyttende system kan være et hvilket som helst datasystem, node eller datamaskin som er i besittelse av hele datasettet som skal signeres. For eksempel kan det signaturbenyttende system være brukerens PC som har mottatt et dokument som krever en signatur.

De kompilerte data overføres så (3) til en liten kryptografitilpasset anordning benyttet av brukeren, for eksempel en WAP-telefon. Brukeren signerer denne meldingen ved å benytte en passende signaturalgoritme. Brukeren gjennomfører så signeringen ved å legge inn en bestemt signerings PIN-kode.

Resultatet sendes tilbake (4) til det signaturbenyttende system, og kompileres inn i en melding som skal sendes (5) til det signaturmottagende system som inneholder i det minste (ref. figur 2):

1) OriginalData og hashalgoritmeidentifikatoren.

2) ToBeSignedMessage, signaturalgoritmeidentifikatoren og signaturen.

OriginalData er den opprinnelige data som skal signeres. Dette kan være dokumenter, protokollstrukturer, kontrakter etc. Den foreliggende oppfinnelse muliggjør en kryptografisk binding mellom disse dataene og brukeren av anordningen.

ToBeSignedMessage er meldingen som presenteres for signering. Den er utsatt for begrensningene i anordningen med hensyn til lengden av dataene som skal signeres. Den består av to deler:

1) En del som brukeren av anordningen kan forstå og som er en del av OriginalData. Fremgangsmåter for å trekke ut lesbar informasjon fra OriginalData kan defineres avhengig av dens egenskaper.

   Hvis egenskapene til OriginalData er slik at ingen lesbar data kan trekkes ut, genererer det signaturbenyttende system en passende tekst for presentasjon til brukeren. Det signaturmottagende system må kunne vite reglene som er benyttet for å selektere denne tekst.

   Hvis anordningen benyttes for å signere for eksempel større dokumenter som inneholder bilder etc., kan dette feltet inneholde dynamisk informasjon om dokumentet. Eksempler er: Doc name=This year budget, Doc no=1FR2, Doc rev=A2, Doc size=2345, Pic1 format=jpeg, Pic1 size=123, Table1 size=234.
   Hvis anordningen benyttes for å signere et bilde eller en musikkfil, kan eksempelinformasjonen være: Title=Dance music vol1, Format=mp3, Size=2345, Length=1.16

2) En del som ikke er forståelig for brukeren av anordningen. Dette er hash-koden til OriginalData. Tilstedeværelsen av hash-koden er den faktiske bindingen mellom de opprinnelige data og signeringen. Den garanterer at brukeren faktisk signerer de opprinnelige data, slik han/hun kjenne dem, og ikke bare den lesbare tekst. Hvis de opprinnelige data utsettes for selv en mindre endring før hash-koding, vil hash-koden se fullstendig annerledes ut enn forventet og brukerens kryptografitilpassede anordning vil kunne vite at dataene har blitt endret og dermed avvise dem.

Denne løsningen presenterer for anordningens bruker en forståelig melding generert fra informasjonen som skal signe-

res. Den er også fleksibel i å gi forskjellige signaturmottagende systemer skreddersydde data som autentiserer både det signaturbenyttende system og anordningens bruker.

Signeringsprosedyren og datasammenstillingen kan implementeres ved å benytte forskjellige typer protokoller. Figur 4 viser et eksempel på en "push"-signeringsforespørsel hvor WML Script benyttes i kommunikasjon med en WAP 1.2 mobil anordning i signeringsprosedyren, og hvor HTTP benyttes mellom det signaturbenyttende og signaturmottagende system. Andre script, protokoller og signeringsanordninger kan imidlertid benyttes for disse formål (for eksempel LDAP [LDAP], SQL [SQL], I-MODE tilpassede anordninger og script).

Til slutt viser figur 5 et eksempel på hvordan de kompilerte forståelige dataene (referert til som ToBeSignedMessage i figur 2 og kompilerte data i figur 3) kan fremstå for brukeren på displayet i den kryptografitilpassede anordning.

Hovedfordelen ved den foreliggende oppfinnelse er at den gjør brukeren i stand til å forstå hva hun/han signerer selv på små og hardwarebegrensede anordninger. Dette øker den signerende parts bevegelsesfrihet, da han/hun kan benytte portable kryptografitilpassede anordninger selv for store datamengder.

En ytterligere fordel er at bare en mindre datamengde sendes til og fra anordningen så vel som prosessert i anordningen, noe som gjør prosedyren raskere og ikke begrenset av verken liten overføringskapasitet eller lav prosessorkapabilitet.

Store ustrukturerte informasjonsbiter kan da bli brutt ned til en definert melding hvis struktur er avtalt, verifisert og deretter signert med brukerens personlige signeringsanordning.

Videre gjør den foreliggende oppfinnelse det mulig å benytte en liten anordning til å signere for eksempel dokumenter og grafisk innhold selv om anordningen ikke er utstyrt med en grafisk skjerm.

Enda en annen fordel ved den foreliggende oppfinnelse er at den gjør det mulig at brukerens private nøkkel kan være atskilt fra det signaturbenyttende system til hvilken det generelle eksterne nett er koblet (for eksempel PC-er til Internett). Risikoen for at inntrengere får tak i de private signeringsnøkler blir følgelig redusert.

Enda en fordel ved oppfinnelsen er at ingen tilpasninger kreves i vanlig signeringsanordninger slik som WAP 1.2 mobilanordninger. Signeringsapplikasjoner som allerede er implementert kan benyttes.

Den foreliggende oppfinnelse er nyttig for WAP 1.2 signText() funksjonalitet eller kryptografiske signeringsapplikasjoner som er implementert ved benyttelse av SIM Application Toolkit (SAT), og dette er benyttet i eksemplene som her er beskrevet. Andre utførelser kan imidlertid også benyttes i scenarioer hvor data må signeres og forstås av mennesker som benytter en liten kryptografianordning og som befinner seg innenfor oppfinnelsens område slik den er definert i det påfølgende selvstendige krav.

Referanser

[PKCS#1] RSA Cryptography Standard
http://www.rsasecurity.com/rsalabs/pkcs/

[PKCS#7] Cryptographic Message Syntax Standard
http://www.rsasecurity.com/rsalabs/pkcs/

[WAPArch] "WAP Architecture Specification"
http://www.wapforum.org/what/technical.htm

[WML] "Wireless Markup Language", WAP Forum
http://www.wapforum.org/what/technical.htm

[WMLScript] "WMLScript Language Specification", WAP Forum
http://www.wapforum.org/what/technical.htm

[WMLCrypto] "WMLScript Crypto Library Specification", WAP Forum
http://www.wapforum.org/what/technical.htm

[HTTP] HyperText Transfer Protocol
RFC 2069
http://www.ietf.org/rfc/rfc2068

[LDAP] Lightweight Directory Access Protocol
RFC 2559
http://www.ietf.org/rfc/rfc2559

[SQL] Structured Query Language
http://www.sql.org

P a t e n t k r a v

1. Fremgangsmåte for elektronisk og/eller digital signering av data ved å benytte en første håndholdte signeringsanordning som benytter et elektronisk signeringssystem bestående av følgende trinn:

a) å trekke ut en del av nevnte data i en andre signeringsanordning,
c) å hash-kode nevnte data i nevnte andre signeringsanordning som resulterer i en hash-kode av nevnte data,
d) å overføre nevnte del av dataene og nevnte hash-kode til nevnte første håndholdte signeringsanordning i en forespørsel,

e) å signere nevnte forespørsel i nevnte første håndholdte signeringsanordning i henhold til nevnte elektroniske signeringssystem,
k a r a k t e r i s e r t v e d følgende trinn etter trinn a) og før trinn c):

b) å kompilere nevnte del av dataene til et format som er tilpasset nevnte første håndholdte signeringsanordning og som er lesbar for en bruker av denne.

2. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at den videre omfatter følgende trinn:
å returnere en signatur som et resultat av nevnte signering fra den første håndholdte signeringsanordning til den andre signeringsanordning.

3. Fremgangsmåte ifølge krav 2,
k a r a k t e r i s e r t v e d at den videre omfatter følgende trinn:

å overføre nevnte data, forespørsel og signatur fra nevnte andre signeringsanordning til en tredje signeringsanordning.

4. Fremgangsmåte ifølge et av de foregående krav, k a r a k t e r i s e r t v e d at den første håndholdte signeringsanordning er en liten kryptografitilpasset anordning som benytter en bestemt protokoll, og at den andre signeringsanordning er et signaturbenyttende system som er tilpasset til å kompilere nevnte del av dataene til nevnte protokoll.

5. Fremgangsmåte ifølge krav 3 eller 4, k a r a k t e r i s e r t v e d at nevnte tredje signeringsanordning er en signaturmottagende anordning for i det minste prosessering, verifisering og/eller lagring av signerte data.

6. Fremgangsmåte ifølge krav 4 eller 5, k a r a k t e r i s e r t v e d at nevnte protokoll er WAP (Wireless Application Protocol) og den første håndholdte signeringsanordning er en WAP-telefon.

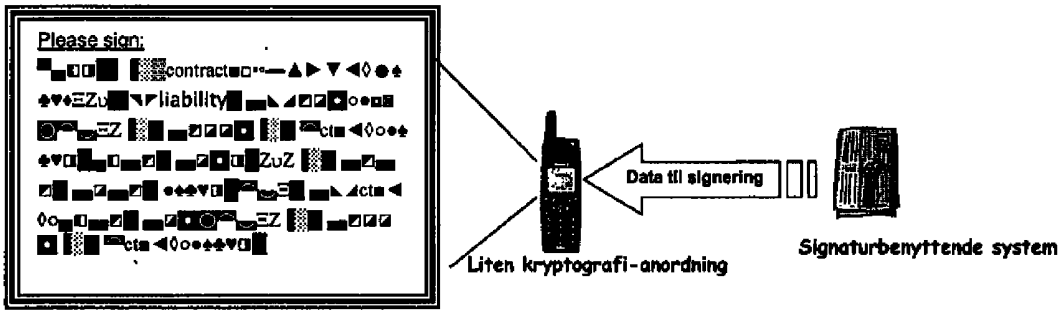
7. Fremgangsmåte ifølge et av de foregående krav, k a r a k t e r i s e r t v e d at nevnte elektroniske signeringssystem benytter private/offentlige nøkler.

8. Fremgangsmåte ifølge et av de foregående krav, k a r a k t e r i s e r t v e d at nevnte data er et dokument, et skjema, en avtale eller en transaksjon.

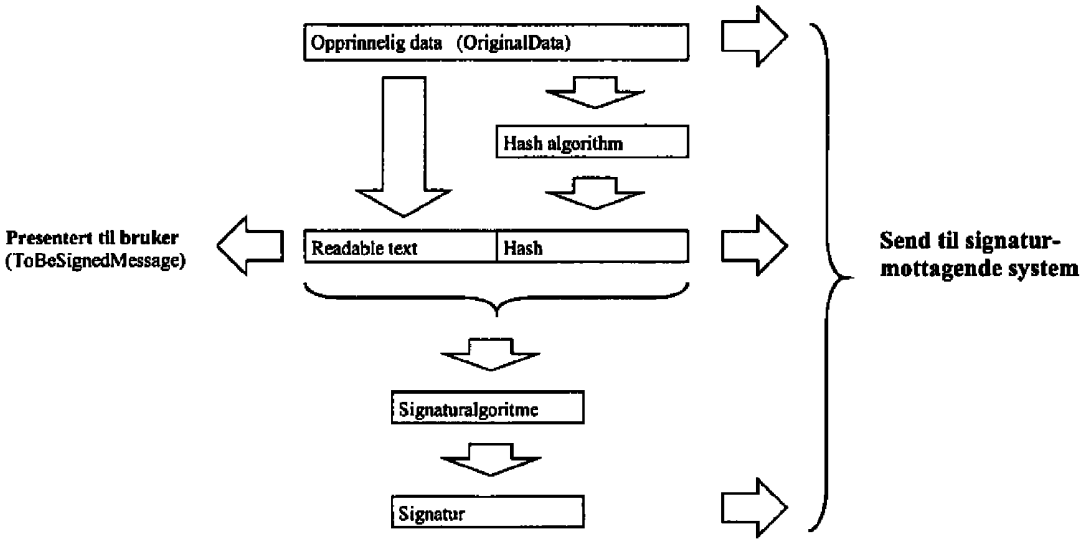
9. Fremgangsmåte ifølge et av kravene 6-8, k a r a k t e r i s e r t v e d at signeringen gjennomføres ved hjelp av WAP 1.2 signText() funksjonalitet.

10. Fremgangsmåte ifølge et av kravene 6-9, k a r a k t e r i s e r t v e d at signeringen gjennomføres ved hjelp av en kryptografisk signeringsapplikasjon

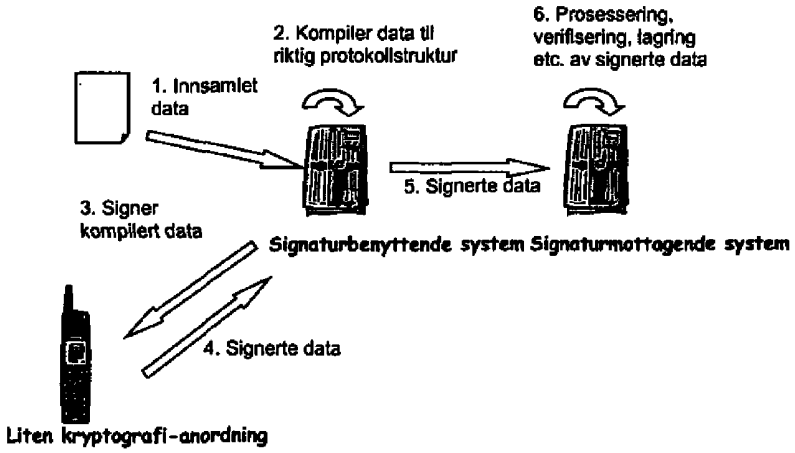
som implementeres ved å benytte SIM Application Toolkit (SAT).



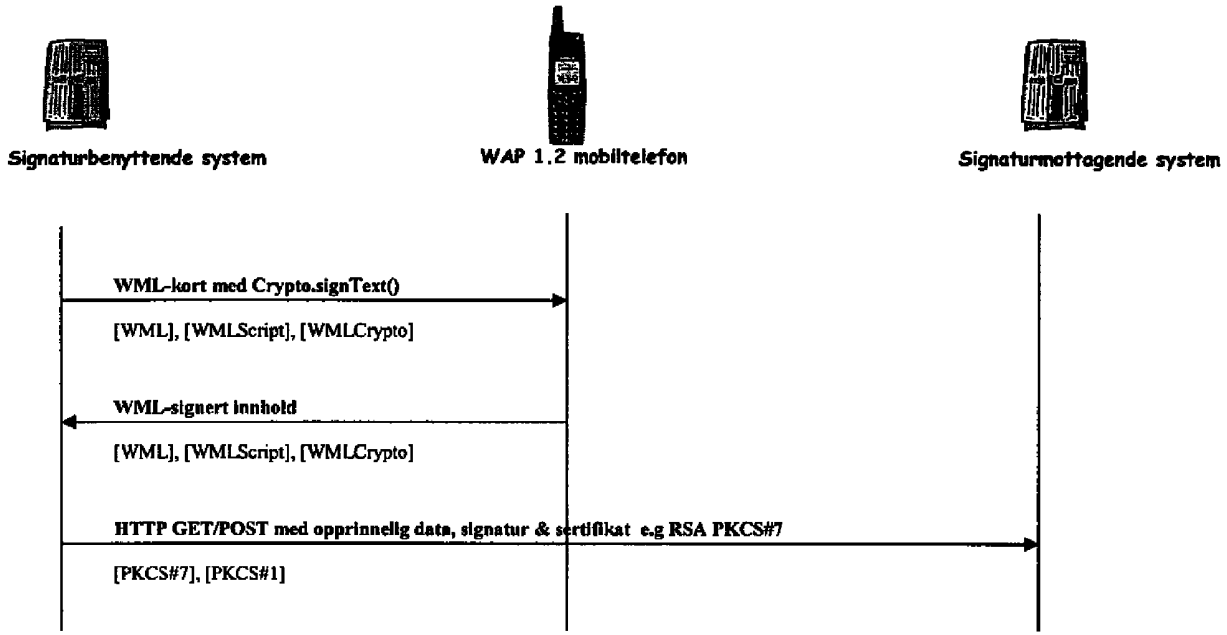
Figur 1 Problem ved signering av ikke-lesbar tekst



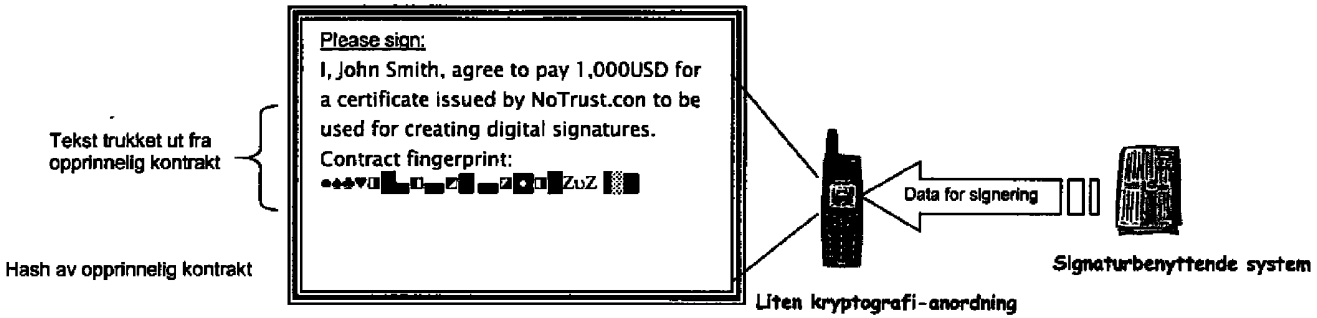
Figur 2 Konstruering av melding som skal sendes til det signaturmottagende system



Figur 3 Videresending av data



Figur 4 Eksempel på en push-signeringsforespørsel som benytter en WAP 1.2 mobiltelefon hvor HTTP benyttes mellom signaturbenyttende og signaturmottagende system.



Figur 5 Eksempel på å kjøpe et sertifikat fra en CA