

(19)



Bureau voor de
Industriële Eigendom
Nederland

(11) 1008044

(12) C OCTROOI²⁰

(21) Aanvraag om octrooi: 1008044

(22) Ingediend: 16.01.98

(51) Int.Cl.⁸
H04L9/32, H04L9/08

(41) Ingeschreven:
19.07.99

(47) Dagtekening:
19.07.99

(45) Uitgegeven:
01.09.99 I.E. 99/09

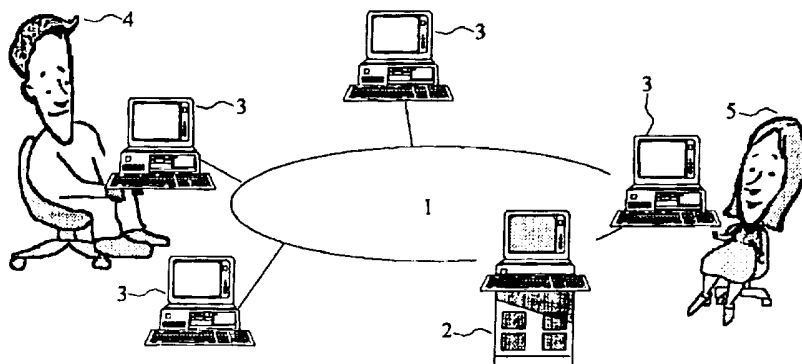
(73) Octrooihouder(s):
Koninklijke KPN N.V. te Groningen.

(72) Uitvinder(s):
Jacobus Theodorus Willem Quak te Den Haag
Eoghan Colm Cathal Sheedy te Den Haag

(74) Gemachtigde:
Geen

(54) Sleutelbeheersysteem.

(57) Beheersysteem voor cryptografische sleutels. In een beheersserver (2) zijn per gebruiker (4, 5) een private (PrK) en een publieke sleutel (PuK) opgeslagen. Ook de server zelf heeft een private en publieke sleutel, voor het authenticeren van te verzenden cryptografische sleutels. Bij compromittering van de private server-sleutel, stuurt de server daarvan bericht aan elke gebruiker, geauthenticeerd met behulp van de private of een geheime sleutel van de gebruiker of terminal. Het bericht omvat een kopie van een nieuwe publieke sleutel van de server. De terminals kunnen berichten detecteren die gewaarmerkt zijn met behulp van die private of geheime sleutel (code) van de gebruiker, waarna de opgeslagen kopie van de oude publieke sleutel vervangen wordt door de in het bericht gedetecteerde kopie van de nieuwe sleutel van de server.



NL C 1008044

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventueel tekeningen.

Sleutelbeheersysteem

ACHTERGROND VAN DE UITVINDING

De uitvinding betreft een beheersysteem voor cryptografische sleutels. Er bestaan voor de beveiliging van elektronische

5 communicatie twee cryptografische technieken: geheime sleutel (SK) systemen die met paren identieke, geheime sleutels (codes) werken en publieke/private sleutel (PrPuK) systemen die met paren bij elkaar horende, niet-identieke sleutels werken. PrPuK systemen worden met name gebruikt wanneer de communicatiepartners elkaar
10 tevoren niet kennen, zoals bij grote groepen gebruikers.

In PrPuK systemen heeft elke gebruiker een private ("geheime") sleutel (PrK) en een daarbij behorende publieke sleutel (PuK). DuKs van de verschillende gebruikers zijn bijvoorbeeld bij een "Trusted Third Party" (TTP), geïncorporeerd in een TTP server (SV),
15 vrijelijk beschikbaar. De PrK is in principe alleen aan de gebruiker bekend. Gesteld dat een gebruiker A en een gebruiker B geregistreerd zijn bij een server SV1. Gebruiker A heeft een private sleutel, PrKa, terwijl zijn publieke sleutel, PuKa, in de server SV1 is opgeslagen. Gebruiker B heeft ook een private
20 sleutel, PrKb, terwijl zijn publieke sleutel ook in de server SV1 is opgeslagen. Ook de private sleutels kunnen in de server bewaard worden, ten behoeve van backup voor de gebruiker, continuïteit overwegingen in een bedrijfsomgeving of vanwege wettelijke verplichtingen. De server stelt certificaten van de publieke
25 gebruikerssleutels PuKa, PuKb, etc., ter beschikking. Een kopie van een PrK wordt alleen verstrekt aan de gebruiker van wie die PrK is, bijvoorbeeld in het geval de gebruiker zijn PrK kwijt is geraakt. Het is denkbaar dat onder bepaalde, wettelijk vastgelegde omstandigheden het een (gouvernementele) veiligheidsorganisatie is
30 toegestaan bij de TTP van een gecijferde tekst de ontcijferde versie op te vragen; in dat geval maakt de TTP gebruik van een opgeslagen PrK. Een derde geval is wanneer een medewerker zijn bedrijf verlaat en gecijferde teksten achterlaat. De in de server aanwezige kopie van de PrK stelt het bedrijf dan in staat deze
35 teksten te ontcijferen.

Een verzoek, door een gebruiker A, om toezending van de PuK van een bepaalde gebruiker B wordt door de TTP server gehonoreerd door

toezending van een certificaat van de gevraagde PuK, PuKb. Dat certificaat omvat de PuK van de gebruiker, voorzien van een digitale handtekening, gebruikmakend van de PrK van de server; dergelijke sleutelcertificaten worden hierna voorgesteld als:

- 5 {PuKa}PrKsv1, {PuKb}PrKsv1, etc., waarin PrKsv1 de private sleutel van server SV1 voorstelt. De digitale handtekening die, ter authenticatie van de afzender, aan het een bericht wordt toegevoegd, wordt gevormd door vercijfering met de PrK van de verzender van de "plain text" van het bericht zelf of, waar
- 10 doorgaans in verband met de verwerkingssnelheid de voorkeur aan wordt gegeven, door vercijfering van een (binaire) samenvatting van dat bericht, "hash" of "digest" genoemd (er zijn voor het produceren daarvan standaard, uit de literatuur bekende algoritmes). De ontvanger van een bericht ontcijfert de als
- 15 handtekening dienende vercijferde "plain text" of "hash" met de publieke sleutel van de verzender. Als het resultaat accoord is is het bericht blijkbaar afkomstig van de eigenaar van die publieke sleutel, de veronderstelde afzender. Wellicht ten overvloede: als een bericht vercijferd moet worden verzonden, dan wordt het
- 20 vercijferd met de publieke sleutel van de ontvangende partij, die het bericht dan weer met zijn eigen private sleutel kan ontcijferen. Een aan een (al of niet vercijferd) bericht toegevoegde elektronische handtekening bestaat uit een copie of binaire samenvatting van dat bericht ("hash"), vercijferd met de
- 25 private sleutel van de verzender; de ontvangende partij ontcijfert de elektronische handtekening dan met de publieke sleutel van de verzender.

- Op de beschreven wijze kunnen gebruikers over PuKs beschikken die gecertificeerd zijn door middel van de digitale handtekening van de
- 30 TTP-server waardoor de integriteit van de toegezonden PuK gegarandeerd is. Door middel van de publieke sleutel van de server, PuKsv1, die aan elke bij SV1 geregistreerde de gebruiker ter beschikking is gesteld, kan bijvoorbeeld gebruiker A uit het ontvangen sleutelcertificaat {PuKb}PrKsv1 PuKb extraheren:
- 35 $PuKb = \{ \{PuKb\}PrKsv1 \} PuKsv1$, om vervolgens een aan gebruiker B te verzenden bericht met PuKb te kunnen vercijferen. Dat vercijferde

bericht kan vervolgens door (alleen) gebruiker B worden ontcijferd door middel van zijn PrK, PrKb.

In een TTP systeem als hierboven beschreven, ontvangen gebruikers dus sleutelcertificaten die op authenticiteit zijn gewaarmerkt

- 5 (geauthenticeerd) door middel van de PrK van de TTP-server ook wel Certification Authority, CA, genoemd. Een probleem ontstaat als op zeker moment de PrK van de CA gecompromitteerd of onbruikbaar raakt. Het gevolg is dat vanaf dat moment de CA geen (betrouwbare) sleutelcertificaten kan afgeven. De gebruikers van de TTP-server
10 moeten daarvan --op betrouwbare wijze-- op de hoogte worden gesteld. Voorts moet aan de gebruikers ook een nieuwe PuK worden toegezonden, afgeleid van een in de TTP-server nieuw gegenereerde PrK. Het probleem is dat deze informatie niet betrouwbaar kan worden verzonden als daarbij de oude PrK van de CA voor het
15 vervaardigen van een elektronische handtekening, wordt gebruikt.

SAMENVATTING VAN DE UITVINDING

- De onderhavige uitvinding voorziet in een methode en systeem ter ondervanging van het in het voorgaande gestelde probleem, namelijk het op betrouwbare wijze aan gebruikers zenden van een bericht dat
20 de PrK van de CA (TTP-server) gecompromitteerd is geraakt. De uitvinding gaat ervan uit dat van de gebruikers niet alleen de PuKs in de TTP-server zijn opgeslagen, maar ook de PrKs. Volgens de uitvinding wordt van die in de TTP-server opgeslagen gebruikers-PrKs gebruik gemaakt door, na het gecompromitteerd raken van de de
25 PuK van de TTP, elke gebruiker, van wie de eigen sleutel PrK niet als gecompromitteerd bekend is, een (electronisch) bericht te zenden dat, in plaats van met de PrK van de TTP, gewaarmerkt is met de private sleutel (PrK) van die gebruiker. Dat waarmerken geschiedt, zoals reeds is aangeduid, door vercijfering van het
30 bericht zelf of van een code ("hash", "digest") die op een standaard wijze van het bericht is afgeleid. Gelieve er nota van te nemen dat normaliter een bericht aan een gebruiker niet met de PrK maar met de PuK van de gebruiker vercijferd wordt.

- De nieuwe PuK van de TTP kan op gelijke wijze, aan de gebruiker
35 overgedragen. Elke gebruiker kan de aldus van de TTP-server ontvangen informatie ontcijferen met behulp van zijn eigen PuK en weet daardoor zeker dat, daar alleen de TTP in het bezit is van een

exemplaar van de PrK van de gebruiker, het bericht van de TTP afkomstig is; dat geldt ook voor de op gelijke wijze toegezonden TTP-PuK.

- Bij voorkeur omvat de software van de gebruikers een module die
- 5 detecteert of een ontvangen bericht, i.c. vanuit de TTP-server, met de PrK van de gebruiker vercijferd/gewaarmerkt is. Als de module dat detecteert, moet de gebruikerssoftware zijn instellingen wijzigen ten aanzien van de PuK van de TTP.

UITVOERINGSVOORBEELDEN

- 10 Figuur 1 toont een netwerk 1, een netwerkserver 2, die tevens als TTP-server dient, en een aantal terminals 3 waarop gebruikers 4 en 5 domicilie hebben gekozen. Berichten worden vercijferd uitgewisseld. Gebruiker 4 die een bericht (MSG4) naar gebruiker 5 wil verzenden, vercijfert dat bericht met de publieke sleutel van
- 15 gebruiker 5, PuK5. De voor vercijfering benodigde PuK van gebruiker 5, PuK5, kan door gebruiker 4 worden verkregen door middel van het bij de server 2 opvragen van een certificaat van PuK5: {PuK5}PrK2, waarin PrK2 de private sleutel van de server 2 is. Als ontcijfering van {PuK5}PrK2 met de publieke sleutel van de server, PuK2,
- 20 succesvol is, weet gebruiker 4 dat de sleutel PuK5 inderdaad van server 2 afkomstig is.
- Nadat het met PuK5 vercijferde bericht ({MSG4}PuK5) via het netwerk 1 bij de gebruiker 5 is angekommen, kan deze (als enige) het bericht ontcijferen met behulp van haar private sleutel, PrK5. Op
- 25 gelijke wijze kan gebruiker 5 een bericht (MSG5) vercijferen met de publieke sleutel PuK4 van gebruiker 4, ontleend aan een van server 2 ontvangen certificaat ({PuK}PrK2). Het vercijferde bericht ({MSG5}PuK4) kan door gebruiker 4 worden ontcijferd met behulp van zijn PrK, PrK4. Bij voorkeur omvat de gebruikerssoftware in de
- 30 terminals 3 een module om bij verzending van een bericht bij de server 2 het certificaat van de actuele PuK van de geadresseerde op te vragen, daaruit de PuK van de geadresseerde te berekenen, het bericht met die berekende PuK te vercijferen en het vercijferde bericht te verzenden.
- 35 Als door de een of andere oorzaak de PrK van server 2, PrK2, niet meer betrouwbaar of bruikbaar is, kan deze niet meer worden gebruikt voor afzender-authenticatie ("electronische handtekening")

bij de overdracht van publieke sleutels van de server naar de gebruikers. Veilige overdracht kan pas weer worden gegarandeerd als bij de server 2 een nieuwe PrK2 is gegenereerd en als de daarbij behorende PuK2 naar de gebruikers gedistribueerd is. Die

5 distributie dient ook veilig te geschieden. Daarbij kan echter de oude PrK2/PuK2 -combinatie niet meer worden gebruikt, daar immers de PrK2 onbetrouwbaar of onbruikbaar is geworden. De combinatie van de nieuwe waarde van PrK2, PrK2', en bijbehorende nieuwe waarde voor PuK2, PuK2', kan ook niet worden gebruikt daar de gebruikers
10 nog niet in het bezit van PuK2' zijn.

Conform de uitvinding wordt nu het volgende gedaan. De server 2 verzendt aan elk gebruiker een bericht, vercijferd of althans gewaarmerkt met behulp van de PrK van de ontvanger: voor gebruiker 4 wordt het bericht gewaarmerkt (geauthenticeerd) met behulp van
15 PrK4, voor gebruiker 5 met behulp van PrK5. Gebruiker 4 kan dat bericht ontcijferen met zijn publieke sleutel, PuK4, gebruiker 5 met PuK5. Ook andere gebruikers zouden dat bericht kunnen ontcijferen, immers met de publieke sleutel van gebruiker 4, maar dat is in dit geval niet erg, immers het bericht wordt toch aan
20 alle gebruikers gedistribueerd en de inhoud is op zich niet geheim. Wel wordt hiermee bereikt dat het bericht gewaarmerkt is als afkomstig van de server 2, immers alleen server 2 kan, buiten gebruiker 4, beschikken over PrK4; PrK4 wordt dus hier gebruikt voor authenticatie in plaats van de gecompromitteerde PrKs. Evenzo
25 wordt aan gebruiker 5 bericht gezonden, geauthenticeerd met behulp van PrK5, en op gelijke wijze naar elke gebruiker die bij server 2 als netwerkgebruiker geregistreerd is. Tezamen met het naar de gebruikers verzonden bericht wordt ook de nieuwe PuK van server 2, PuK2, --die simultaan wordt gegenereerd met de nieuwe waarde voor
30 PrK2-- aan alle gebruikers overgedragen. Ook daarbij geldt dat die nieuwe waarde van PuK2 gewaarmerkt (geauthenticeerd) is met behulp van de PrK van de gebruiker.

Opgemerkt wordt dat, algemeen gesteld, volgens de uitvinding voor authenticatie gebruik wordt gemaakt van een gegeven dat bekend is
35 aan de zendende zijde en dat aan de ontvangende zijde op echtheid (authenticiteit) kan worden geverifieerd. In het voorgaande wordt voorgesteld om in normale situaties voor authenticatie gebruik te

maken van de private sleutel van de zendende partij, server 2, die door middel van de bij de ontvangende partij, gebruiker 4 of 5, kan worden getest op echtheid. In uitzonderingssituaties wordt niet de private sleutel van de server 2, maar de private sleutel van de gebruiker gebruikt, die eveneens door de gebruiker (elke gebruiker afzonderlijk) kan worden getest op echtheid. In het algemeen kan ook van een ander gegeven gebruik worden gemaakt dat aan de zijde van de server 2 aanwezig is, niet publiek is en door de gebruikers kan worden getest op echtheid. Van belang daarbij is dat het gegeven niet publiek, maar slechts "bilateraal" (alleen bij de server en één gebruiker) bekend is. Het is dus ook mogelijk om, in plaats van de private sleutel van de gebruiker, een ander gegeven te gebruiken. Een dergelijk gegeven kan speciaal voor het doel dat in het bovenstaande wordt beschreven, namelijk betrouwbare communicatie tussen de server en de gebruikers in geval de private sleutel van de server gecompromitteerd raakt, tevoren in de server en de gebruikersterminal worden ingebracht. Bijvoorbeeld kan de server 2 een voor elke afzonderlijke terminal 3 unieke (geheime) terminalcode genereren die, vercijferd met een publieke terminalsleutel (PuK3), naar de terminal wordt gezonden en daar, na (door de terminal) te zijn ontcijferd met de private sleutel (PrK3) van die terminal, wordt opgeslagen. Bij het gecompromitteerd raken van PrK2 kan het bericht daarvan en de waarde van de nieuwe publieke serversleutel vercijferd worden met de in de server opgeslagen geheime terminalcode. Aan terminalzijde kan het bericht en de nieuwe waarde voor PuK2 met dezelfde geheime terminalcode, die immers ook in de terminal is opgeslagen, worden ontcijferd. De geheime terminalcode, opgeslagen in zowel de server als de terminal, fungeert dus als geheime sleutel binnen een (ad hoc) SK systeem tussen de server en de terminal.

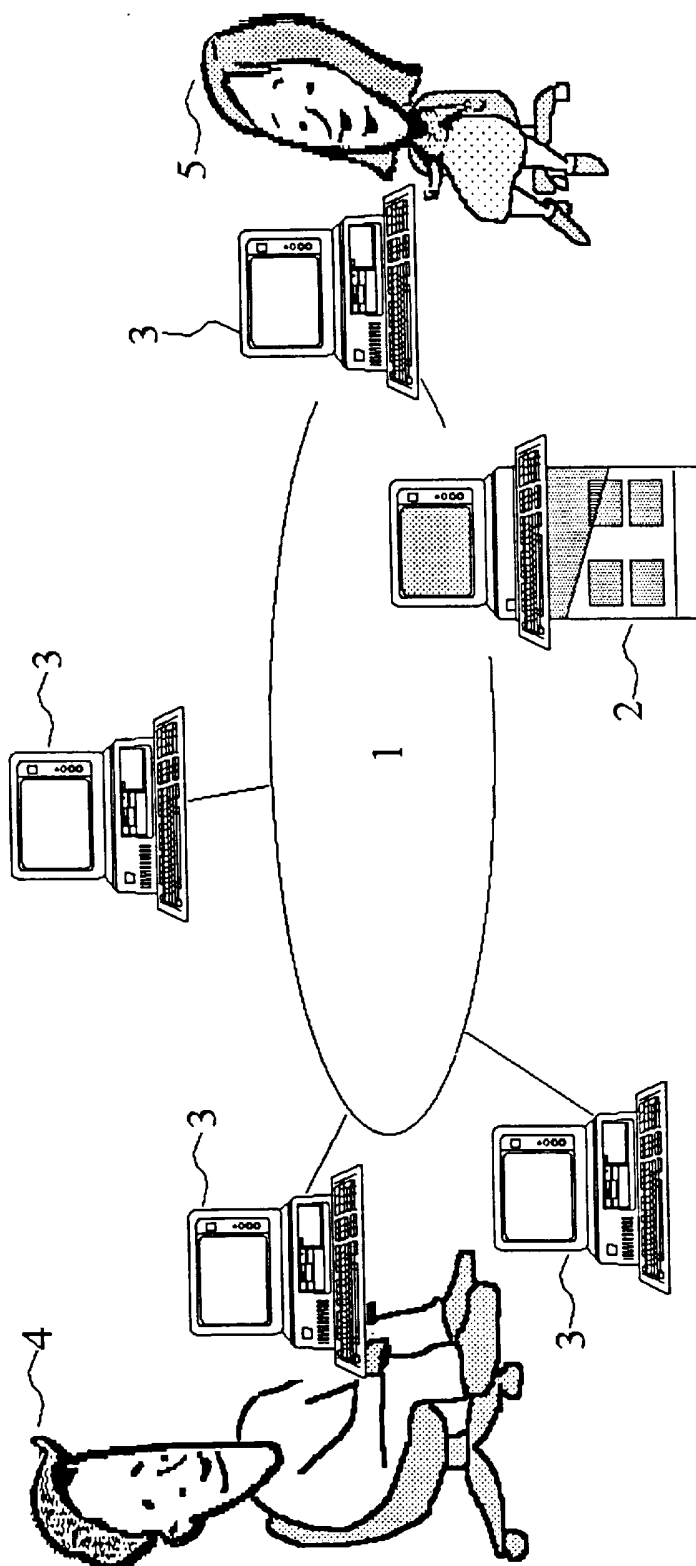
Verder wordt opgemerkt dat, waar in het voorgaande gebruikt wordt gemaakt van de PrK resp. PuK van de gebruiker (die de gebruiker via een persoonlijke token of smart card of op een andere wijze in de terminal invoert, waardoor die voor kortere of langere tijd in de terminal resideren), het op gelijke wijze mogelijk is een PrK resp. PuK van de terminal zelf te gebruiken (die in principe permanent in de terminal resideren).

CONCLUSIES

1. Beheersysteem voor cryptografische sleutels, omvattende een server (2) die middelen omvat voor het via gebruikersterminals (3), waarop gebruikers (4, 5) domicilie kunnen kiezen, en een datanetwerk (1) ontvangen, opslaan en uitgeven van cryptografische sleutels, te weten per gebruiker of terminal een private sleutel (PrK) en een daarbij horende publieke sleutel (PuK), waarbij ook het beheersysteem zelf een eigen private sleutel en bijhorende publieke sleutel heeft, die normaliter gebruikt worden voor het op authenticiteit waarmerken van door de server naar de gebruikers te verzenden berichten en/of cryptografische sleutels, m e t h e t k e n m e r k d a t de server middelen omvat voor het onder omstandigheden aan elke gebruiker overdragen van een bericht dat op authenticiteit gewaarmerkt wordt met behulp van een paar identieke of niet-identieke codes, welk codepaar per gebruiker of gebruikersterminal uniek is en waarbij één code van dat codepaar in de server is opgeslagen en één code in de terminal of bij de gebruiker.
2. Beheersysteem volgens conclusie 1, m e t h e t k e n m e r k d a t het codepaar bestaat uit de private sleutel van de gebruiker of terminal, opgeslagen in de server en de publieke sleutel van de gebruiker of terminal, permanent of tijdelijke opgeslagen in de terminal.
3. Beheersysteem volgens conclusie 2, m e t h e t k e n m e r k d a t het genoemde bericht naar de gebruikers wordt overgedragen indien de private sleutel en de publieke sleutel van de server vervangen zijn door een nieuwe private en publieke sleutel, en dat het bericht een copie van de nieuwe publieke sleutel van de server omvat.
4. Beheersysteem volgens conclusie 3, m e t h e t k e n m e r k d a t de terminals middelen omvatten voor het opslaan van de private sleutel van de gebruiker of terminal en van een copie van de publieke sleutel van de server, alsmede middelen voor het detecteren van berichten die gewaarmerkt zijn met behulp van een sleutel, gelijk aan die private sleutel, alsmede middelen voor het in een zodanig gewaarmerkt bericht detecteren van een copie van de nieuwe publieke sleutel van de server, en voor het vervangen van de

opgeslagen copie van de oude publieke sleutel door de in het
bericht gedetecteerde copie van de nieuwe sleutel van de server.

1008044

FIG. 1

RAPPORT BETREFFENDE
NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFIKATIE VAN DE NATIONALE AANVRAGE		Kenmerk van de aanvrager of van de gemachtigde 402470NE	
Nederlandse aanvraag nr. 1008044		Indieningsdatum 16. januari 1998	
		Ingeroepen voorrangsdatum	
Aanvrager (Naam) KONINKLIJKE PTT NEDERLAND N.V.			
Datum van het verzoek voor een onderzoek van internationaal type		Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr. SN 30638 NL	
I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)			
Volgens de Internationale classificatie (IPC) Int. cl. ⁶ : H 04 L 9/08			
II. ONDERZOCHE GEBIEDEN VAN DE TECHNIEK			
Onderzochte minimum documentatie			
Classificatiesysteem	Classificatiesymbolen		
Int. cl. ⁶	H 04 L		
Onderzochte andere documentatie dan de minimum documentatie voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen			
III. ☐ GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)			
IV. ☐ GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)			

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN
INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek

NL 1008044

A CLASSIFICATIE VAN HET ONDERWERP
IPC 6 H04L9/08

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B ONDERZOCHE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)
IPC 6 H04L

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
Y A	WO 97 18655 A (MICROSOFT) 22 Mei 1997 zie bladzijde 2, regel 19 - bladzijde 3, regel 29 zie bladzijde 9, regel 23 - regel 29 zie bladzijde 13, regel 9 - regel 12 ---	1 3
Y	EP 0 535 863 A (ATT) 7 April 1993 zie bladzijde 3, regel 44 - regel 48 zie bladzijde 4, regel 43 - bladzijde 5, regel 6 --- -/--	1



Verdere documenten worden vermeld in het vervolg van vak C



Leden van dezelfde octroofamilie zijn vermeld in een bijlage

Speciale categorieën van aangehaalde documenten

- "A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang
- "E" eerder document, maar gepubliceerd op de datum van indiening of daarna
- "L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven
- "O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel
- "P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvraag, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octroofamilie

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid

9 Oktober 1998

Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type

Naam en adres van de instantie

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

De bevoegde ambtenaar

Holper, G

C (Vervolg) VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel metaanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	W0 97 31450 A (VISA INTERNATIONAL) 28 Augustus 1997 zie bladzijde 4, laatste alinea zie bladzijde 5, regel 16 - regel 24 zie bladzijde 6, regel 9 - bladzijde 7, regel 15 zie bladzijde 10, regel 1 - bladzijde 15, regel 7 zie bladzijde 19, regel 18 - regel 21 ---	1,3
A	SANTOSH CHOKHANI: "TOWARD A NATINAL PUBLIC KEY INFRASTRUCTURE" IEEE COMMUNICATIONS MAGAZINE, deel 32, nr. 9, 1 September 1994, bladzijden 70-74, XP000476557 NEW YORK (US) zie het gehele document -----	1

**VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN
INTERNATIONAAL TYPE**

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek

NL 1008044

In het rapport genoemd octrooigeschrift		Datum van publicatie	Overeenkomend(e) geschrift(en)		Datum van publicatie
WO 9718655	A	22-05-1997	US 5680458	A	21-10-1997
			AU 1118597	A	05-06-1997
			EP 0861541	A	02-09-1998

EP 535863	A	07-04-1993	US 5241599	A	31-08-1993
			AU 648433	B	21-04-1994
			AU 2351392	A	08-04-1993
			CA 2076252	A	03-04-1993
			JP 2599871	B	16-04-1997
			JP 6169306	A	14-06-1994

WO 9731450	A	28-08-1997	US 5761306	A	02-06-1998
			AU 2137797	A	10-09-1997
