(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 October 2002 (31.10.2002)

PCT

(10) International Publication Number
WO 02/087150 A1

(51) International Patent Classification^7: H04L 9/32

(21) International Application Number: PCT/SE02/00737

(22) International Filing Date: 12 April 2002 (12.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20012029 25 April 2001 (25.04.2001) NO

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TÖNNESLAND, Sverre** [NO/NO]; Etterstadsletta 76, N-0659 Oslo (NO). **BJÖLSETH, Pål** [NO/NO]; Sköyen Terrasse 28, N-0276 Oslo (NO).

(74) Agents: **BOESTAD, Kajsa** et al.; Ericsson AB, Patent Unit Internet Applications, S-164 80 Stockholm (SE).

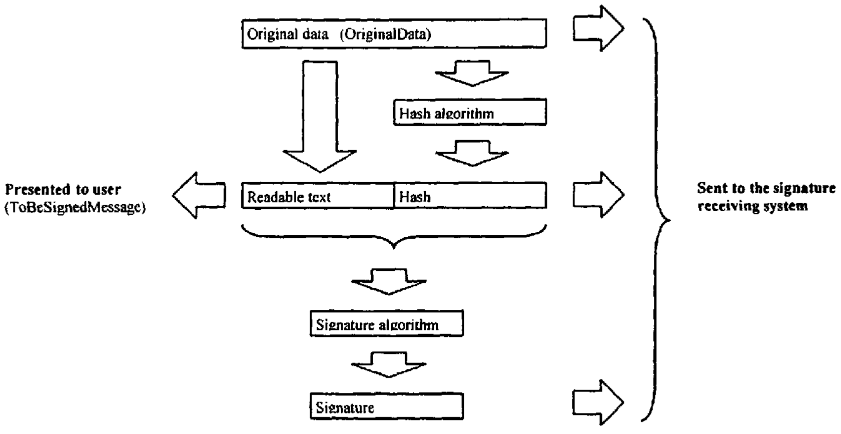
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR NON REPUDIATION USING CRYPTOGRAPHIC SIGNATURES IN SMALL DEVICES


Original data (OriginalData)
Hash algorithm
Presented to user (ToBeSignedMessage)
Readable text
Hash
Sent to the signature receiving system
Signature algorithm
Signature

Construction of the message to be sent to the signature receiving system

(57) Abstract: A method for providing electronical signing of data using a limited signing device is disclosed. This is achieved by extracting a part of the data in a signature using system, compiling it to a proper protocol used by the signing device and transferring it to said signing device together with a hash of the data. The user of the signing device will then be presented to the compiled part of the data which is adjusted according to the limitations of the signing sevice and which is understandable for the user. The user may then electronically sign the data by means of the signing device using an appropriate signature algorithm. A correct hash proves that the user really signs the intended data, aven if he is presented only to an understandable and signing device adjusted part of the data. The resulting signature is returned to the signature using system, and the original data, the part of the data, the hash and the signature are sent to a signature receiving system for processing, verification, storing, etc.

WO 02/087150 A1

Method for non-repudiation using cryptographic signatures in small devices

Field of the invention

The invention is related to networked computing devices, especially when cryptographic signing is being used to achieve non-repudiation, access control, user verification, etc.

Background of the invention

Many kinds of applications, e.g. electronic commerce (e-commerce) or mobile commerce (m-commerce), require the ability to provide persistent proof that someone has authorized a transaction. Also, signing of electronic material, such as assignments, business reports and different kinds of forms is expected to be customary in the near future.

E-commerce and m-commerce are rapidly growing business areas, and both public and private administrations now seem to make adjustments for allowing electronic signing. However, a breakthrough for electronic signing is depended of secure, tamper-proof and simple procedures and solutions. The signing part has to be sure that what he/she is signing is the same as received at the receiving part. The receiving part must be sure of that the signing part is who he/she says he/she is. Further, the signing should be simple without requiring any technical knowledge from the user, and preferably feasible independent of time and localization.

Cryptographic signatures are being used in a multitude of areas. This typically involves in addition to the user, being the owner of the cryptographic signing device, a signature using system and a signature receiving system. The signature using system asks the user to perform a cryptographic signature on the data presented. The user signs and returns the signature back to the signature using system. The signature using system can pass the data that was signed and the signature to the signature receiving system. The signature receiving system has a cryptographically binding relation between what the signature using system presented to the user for signing, and what the user signed.

The PKI (Public Key Infrastructure) is a widely used system for cryptographic signing and authentication, well known by persons skilled in the art. A trusted part in a PKI system issues pairs of electronic keys. The pair consists of one private key and one public key. The private key is only known by the user (or the user's signing device), but the public key may be known by any second part indented to receive signed data from a user. In the user's device, the object to be signed and the private key are inputs to some algorithm outputting the object in a signed condition. At the receiving part, the signed object and the public key are inputs to some other algorithm, extracting the original object from the signed object. The object will be correctly extracted only if the private key signed it. Consequently, the receiving part can be sure that the object was signed by that specific user when utilizing this user's public key for extraction signed the object.

Many electronic devices already support cryptographic signing. One example is a PC with an Internet browser installed. The browser may have one or more certificates containing public keys issued from one or more trusted parts or so-called Certification Authorities (CA).

One problem with this is that a PC usually is bound to one fixed location, and/or it is too big to be carried around everywhere. However, the need for signing materials is not limited to places in which PCs are localized or may be carried.

Further, a PC that is being online all the time or for longer time periods is very vulnerable for data sniffing, and there might be a risk for intruders grabbing the private keys. For security reasons, a user might want to utilize his/hers personal signing device for signing the material presented on the PC.

The solution of the above-mentioned problems might be small portable devices such as cellular phones. "WMLScript Language Specification", WAP Forum describes an implementation of a function allowing WAP phones executing cryptographic signing. The WAP phone requests the user to sign a string of text by entering e.g. a PIN code for the device to cryptographically sign the string.

However, such devices, e.g. cellular phones, are characterized by being memory and processing capacity limited and the cryptographic signing function is accessible through a defined and limited interface.

Further, small devices like cellular phones normally do not have a graphical screen or relatively large programmes like PowerPoint and Word installed.

The problems then occur when the data to be signed is too big to be presented to the user, or in a format that is not understandable to the user or not compatible to the signing device. The above-mentioned WAP specification, however, assumes that the data is understandable and small enough to be presented on hardware and display limited devices.

Summary of the invention

The main object of the present invention is to overcome the above-identified problems and provide non-repudiation between a user, a signature using system and a signature receiving system. This is achieved by a method defined by the enclosed claim 1.

More specifically, the present invention provides a method for digitally signing of data using a signing device by extracting a part of the data in a signature using system, compiling it to a proper protocol used by the signing device and transferring it to said signing device together with a hash of the data. The user of the signing device will then be presented to the compiled part of the data, which is adjusted according to the limitations of the signing device and is understandable for the user. The user may then electronically sign the data by means of the signing device using an appropriate signature algorithm. A correct hash proves that the user really signs the intended data, even if he is presented only to an understandable and adjusted part of the data. The resulting signature is returned to the signature using system, and the original data, the part of the data, the hash and the signature are sent to a signature receiving system for processing, verification, storing, etc.

The present invention allows using small hardware and processor limited signing devices, e.g. mobile phones, for signing data being too large for the signing device.

Brief description of the drawings

Fig. 1 illustrates the problem of signing non-readable text on a small device.

Fig. 2 is a flow chart showing the data flow in an embodiment according to the present invention.

Fig. 3 shows how the data may be transferred between elements involved in an embodiment according to the present invention.

Fig. 4 shows an example of the data flow in a push signing request using a WAP 1.2 enabled mobile device, in which

HTTP is used between a signature using and a signature receiving system.

Fig. 5 is a view of how an extracted text from an original object that is to be signed may look like.

Preferred embodiments of the present invention

In the following, a preferred embodiment of the present invention is described. Note that this embodiment is discussed for illustration purposes only, and does not limit the invention as it is defined in the enclosed claim 1.

The embodiment described provides a flexible way to accomplish cryptographic binding between a user and a set of data that is unreadable to human beings in its original form or too large to be presented to the user for signing. It is partly described in a protocol syntax with reference to the above mentioned drawings.

Figure 3 illustrates a push scenario, where the signature using system connects to the small cryptographic device and conveys the signature request. In a pull scenario, the small cryptographic device connects to the signature using system and asks for the data to be signed.

The signature using system and signature receiving system are logical entities in a computing network. They might reside in the same network component or they might be separated from each other as in the exemplification above where the signature using system is the user's PC.

The signature using system compiles (2) a collected (1) message in such a way that it can be presented and understood by the user. The signature using system may be any data system, node or computer that is being in possession of the entire collected data that is to be signed. For example, the signature using system may be the user's PC having received a document requiring a signature.

The compiled data is then transferred (3) to a small cryptographic enabled device of the user, e.g. a WAP phone. The user signs this message using an appropriate signature algorithm. The user may accomplish the signing by entering a certain signing PIN code.

The result is sent back (4) to the signature using system, and compiled into a message to be sent (5) to the signature receiving system containing at least (ref. fig. 2):

1) OriginalData and hash algorithm identifier.

2) ToBeSignedMessage and the signature algorithm identifier and the signature.

OriginalData is the original data that was to be signed. This can be documents, protocol structures, contracts, etc. The present invention enables a cryptographic binding between this data and the user of the device.

The ToBeSignedMessage is the message presented for signing. It is subject to the limitations in the device regarding length of the data to be signed. It has two parts:

1) A part that the user of the device will understand and that is part of the OriginalData. Methods for extracting readable information from the OriginalData can be defined depending on its nature.

   If the nature of the OriginalData is such that no readable data can be extracted, the signature using system generates a suitable text for presentation to the user.
   The signature receiving system must know the rule used for selecting this text.

If the device is used for signing e.g. large documents containing pictures etc., this field can contain dynamic information about the document. Examples are: Doc name=This years budget, Doc no=1FR2, Doc rev=A2, Doc size=2345, Pic1 format=jpeg, Pic1 size=123, Table1 size=234.
If the device is used for signing a picture or music file, then example information could be: Title=Dance music vol1, Format=mp3, Size=2345, Length=1.16

2) A part that is not understandable to the user of the device. This is the hash of the OriginalData. The presence of the hash is the real binding between the original data and the signing. It guarantees that the user really signs the original data, as he/she knows it, and not just the readable text. If the original data is exposed to only a small change before hashing, the hash will look completely different than expected, and the cryptographic enabled device of the user will know that the data has been changed, and then reject it.

This solution presents to the user of the device an understandable message of which information is to be signed. It is also flexible in providing different signature receiving systems with tailor-made data authenticating both the signature-using system and the user of the device.

The signing procedure and the data collection can be implemented using different kinds of protocols. Figure 4 shows an example of a push-signing request where WML Script is being used in the communication with a WAP 1.2 enabled mobile device during the signing procedure, and where HTTP is used between the signature using and signature receiving systems. However, other scripts, protocols and signing devices can be used for these purposes (e.g. LDAP [LDAP], SQL [SQL], I-MODE adapted devices and scripts).

Finally, fig. 5 views an example of how the compiled understandable data (referred to as ToBeSignedMessage in fig. 2 and compiled data in fig. 3) can appear for the user on the display of the cryptographic enabled device.

The main advantage of the present invention is that it makes the user able to understand what he/she is signing even on small and hardware limited devices. This increases a signing part's freedom of movement, as he/she may use portable cryptographic enabled devices even for large amounts of data.

A further advantage is that only a small amount of the data to be signed is sent to and from the device as well as processed by the device, making the procedure faster and not limited by neither narrow transfer capacity nor low processor capability.

Very large unstructured pieces of information may then be broken down into a defined message agreed upon structure, verified and then signed with the user's personal signing device.

Further, the present invention makes it possible to use a small device to sign e.g. documents with graphical content even if the device is not equipped with a graphical screen.

Still another advantage of the present invention is that it allows the user's private key to be separated from the signature using system to which generally external networks are connected (e.g. PC-s to the Internet). The risk of intruders grabbing private signing keys is consequently reduced.

Still another advantage of the invention is that no adjustments in custom signing devices such as WAP 1.2 enabled mobile devices are required. The sign applications already implemented may be utilized.

The invention is suitable for the WAP 1.2 signText() functionality or a cryptographic sign application implemented using the SIM Application Toolkit (SAT), and this is used in the examples here described. However, other embodiments applicable in any scenarios where data has to be signed and understood by a human using a small cryptographic device being within the scope of the invention as defined by the following claims may be utilized.

References

[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

Patent claims

1. A method for electronically and/or digitally signing of data using a first signing device utilizing an electronic signing system,
characterized in

extracting a part of said data in a second signing device,

hashing said data in said second signing device resulting in a hash of said data,

transferring said part of data and said hash to said irst signing device in a single request,

signing said request in said first signing device according to said electronic signing system.

2. A method according to claim 1,
characterized in that said extracting also includes compiling said parts of data for thereby being adjusted to said first signing device.

3. A method according to claim 1 or 2,
characterized in that said parts of data is readable on said first signing device for a user thereof.

4. A method according to any of the preceding claims,
characterized in that said part of data in the request is user understandable on the first signing device.

5. A method according to any of the preceding claims,
characterized in that it further includes the following step:

returning a signature as a result of said signing from the first signing device to the second signing device.

6. A method according to claim 5, characterized in that it further includes the following step:

transferring said data, request and signature from said second signing device to a third signing device.

7. A method according to any of the preceding claims, characterized in that the first signing device is a small cryptographic enabled device using a certain protocol and the second signing device is a signature using system adjusted to compile said part of data into said protocol.

8. A method according to claim 6 or 7, characterized in that said third signing device is a signature receiving device for at least processing, verification and/or storing of signed data.

9. A method according to claim 7 or 8, characterized in that said protocol is WAP (Wireless Application Protocol) and the signing first device is a WAP enabled mobile device.

10. A method according to any of the preceding claims, characterized in that said electronic signing system is using private/public keys.

11. A method according to any of the preceding claims, characterized in that said data is a document, a form, an assignment, or a transaction.

12. A method according to claim 9-11, characterized in that the signing is executed by means of the WAP 1.2 signText()functionality.

13. A method according to claim 9-11, characterized in that the signing is executed by means of a cryptographic sign application implemented using the SIM Application Toolkit (SAT).

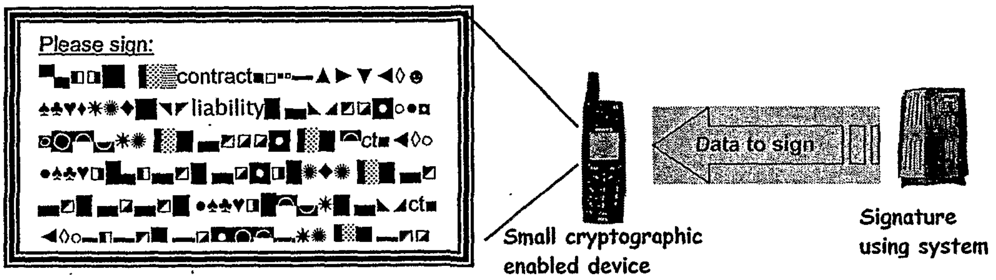


Figure 1 Problem signing non readable text

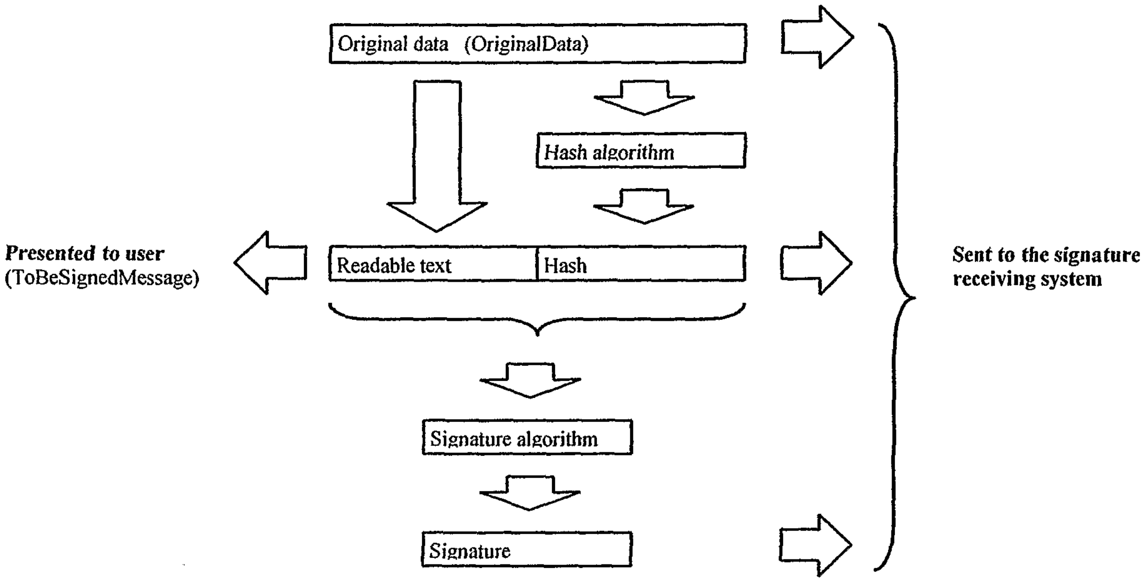


Fig 2. Construction of the message to be sent to the signature receiving system

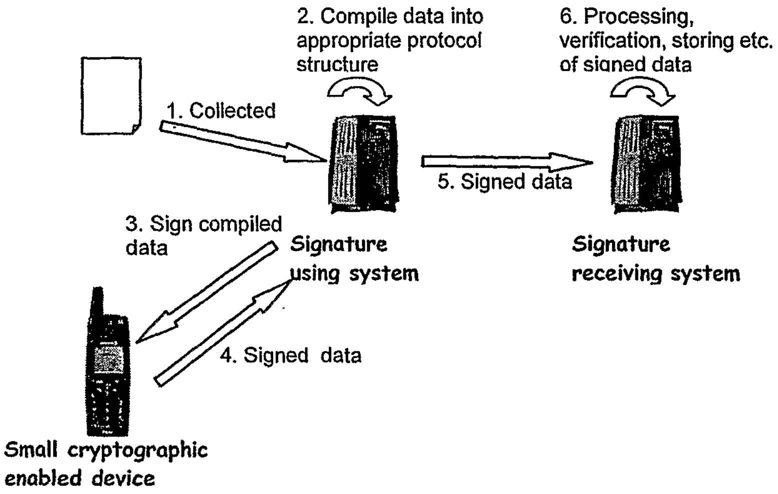

2. Compile data into appropriate protocol structure
6. Processing, verification, storing etc. of sianed data
1. Collected
5. Signed data
3. Sign compiled data
Signature using system
Signature receiving system
4. Signed data
Small cryptographic enabled device

Figure 3 Passing of data to sign/signed data

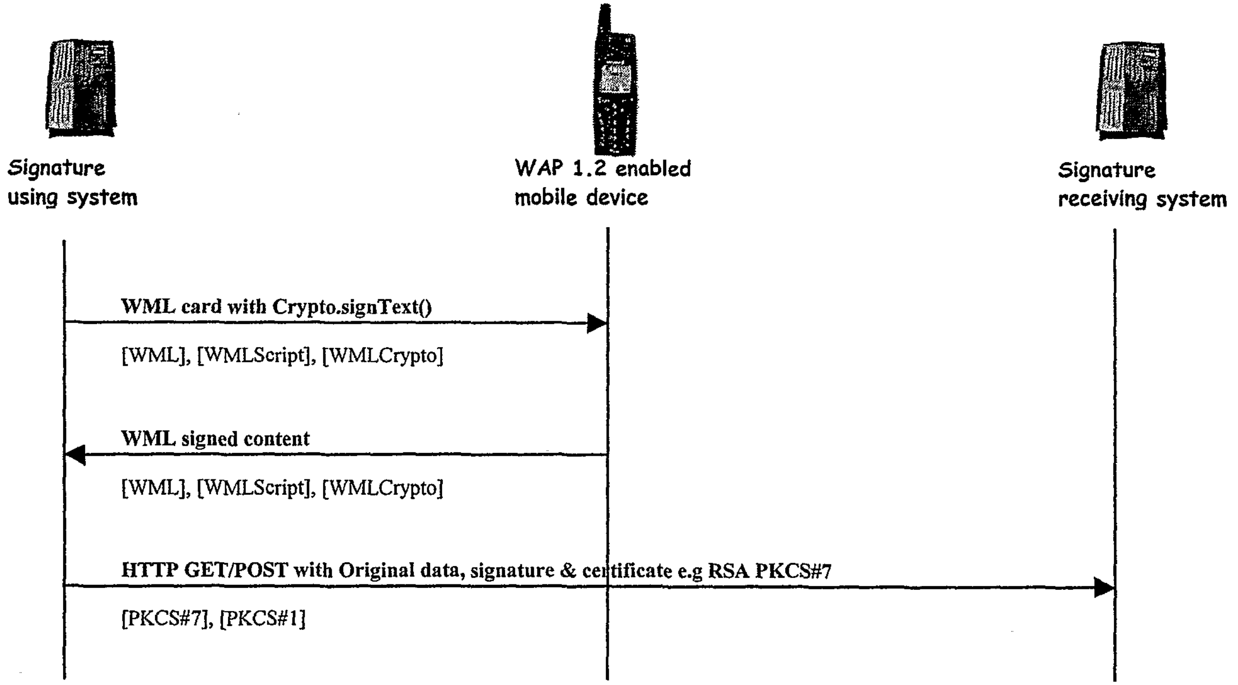
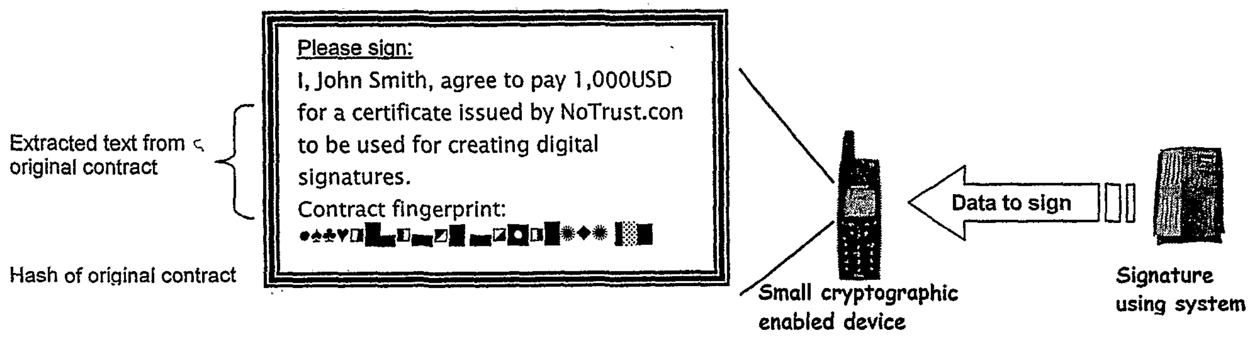

Signature
using system
WAP 1.2 enabled
mobile device
Signature
receiving system
WML card with Crypto.signText()
[WML], [WMLScript], [WMLCrypto]
WML signed content
[WML], [WMLScript], [WMLCrypto]
HTTP GET/POST with Original data, signature & certificate e.g RSA PKCS#7
[PKCS#7], [PKCS#1]

Figure 4 Example of a push signing request using a WAP 1.2 enabled mobile device where HTTP is used between signature using and signature receiving system.



Please sign:
I, John Smith, agree to pay 1,000USD for a certificate issued by NoTrust.con to be used for creating digital signatures.
Contract fingerprint:

Extracted text from original contract
Hash of original contract
Small cryptographic enabled device
Data to sign
Signature using system

Figure 5 Example of buying a certificate from a Certificate Authority

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/00737

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9905819 A1 (CHANTILLEY CORPORATION LIMITED), 4 February 1999 (04.02.99), page 3, line 31 - page 4, line 18, abstract	1-13
	--	
A	WO 0039958 A1 (SONERA OYJ), 6 July 2000 (06.07.00), figure 1, abstract	1-13
	--	
A	EP 0689316 A2 (AT & T CORP), 27 December 1995 (27.12.95), abstract	1-13
	--	

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 25 July 2002	Date of mailing of the international search report 0 5 -08- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/SN Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE 02/00737

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9905819 A1	04/02/99	AU 8453898 A	16/02/99
		EP 0998800 A	10/05/00
		GB 2327831 A	03/02/99
		GB 9715411 D	00/00/00
		JP 2001511544 T	14/08/01
WO 0039958 A1	06/07/00	AU 1984600 A	31/07/00
		CN 1339207 T	06/03/02
		EP 1142194 A	10/10/01
		FI 108373 B	00/00/00
		FI 982728 D	00/00/00
EP 0689316 A2	27/12/95	CA 2149067 A	23/12/95
		JP 8032575 A	02/02/96