

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 July 2009 (23.07.2009)

PCT

(10) International Publication Number
WO 2009/091611 A1

(51) International Patent Classification:
H04L 9/00 (2006.01)

(74) Agent: **RADLO, Edward, J.**; Sonnenschein Nath & Rosenthal LLP, P.O. Box 061080, Wacker Drive Station, Sears Tower, Chicago, IL 60606-1080 (US).

(21) International Application Number:
PCT/US2009/000357

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 16 January 2009 (16.01.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/011,668 18 January 2008 (18.01.2008) US

(71) Applicant (for all designated States except US): **IDEN-TRUST, INC.** [US/US]; 55 Hawthorne Street, Suite 400, San Francisco, CA 94105 (US).

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **EPSTEIN, William, C.** [US/US]; 4391 Parkview Drive, Salt Lake City, UT 84124 (US). **MILLER, Lawrence, R.** [US/US]; 3 Dan Beard Lane, Redding, CT 06896 (US).

[Continued on next page]

(54) Title: BINDING A DIGITAL CERTIFICATE TO MULTIPLE TRUST DOMAINS

1st Embodiment – Self Signed Certificate

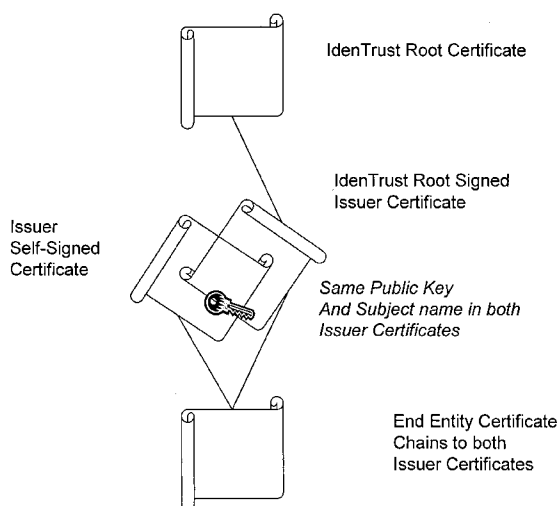


FIG. 2

(57) Abstract: A public key infrastructure comprising a participant that issues digital certificates. Each digital certificate can be relied upon in at least two different trust domains. The public key infrastructure does not employ policy mapping between or among the trust domains. Furthermore, the public key infrastructure does not link any pair of trust domains via cross- certificates. Just one trust domain is bound to the digital certificate at any given moment. The current trust domain that is to be bound to the digital certificate is elected by a relying party at the time of reliance, based upon a specific certificate validation methodology selected by the relying party.

WO 2009/091611 A1



Published:

— *with international search report*

BINDING A DIGITAL CERTIFICATE TO MULTIPLE TRUST DOMAINS

RELATED APPLICATION

The present patent application claims the benefit of, and incorporates by reference,
5 U.S. provisional patent application 61/011,668 filed January 18, 2008, entitled "Binding a Digital Certificate to Multiple Trust Domains".

TECHNICAL FIELD

This invention pertains to the field of public key infrastructures, digital certificates,
10 and public key cryptography.

BACKGROUND ART

Traditionally, digital certificates have been issued within a trust domain "silo" governed by a legal regime presumed to be uniform. Methods involving cross-certification
15 between such trust domains through the use of policy mapping and a bridge certificate authority have permitted a certificate issued within one trust domain to be relied upon in another.

Another approach is to design a hierarchic Public Key Infrastructure in which a Root Certificate Authority ("Root CA") authorizes Subordinate Certificate Authorities ("Sub-
20 CAs") to issue end entity certificates that can be relied upon by any other end entity authorized by Sub-CAs of the Root. One implementation of a hierarchic PKI is the IdenTrust System, which constitutes a single, uniform, trust domain with end entity certificates issued by a global network of Sub-CAs of the IdenTrust Root CA, all operating under uniform standards, policies, procedures and rules.

25 The motivation for the invention was to allow end entity certificates created for use within the IdenTrust System also to be used outside the System, in another trust domain, about which more below.

Most PKI systems are "open" in the sense that they: (1) rely upon local, public, law governing the making and reliance upon digital signatures and the validity of digital
30 certificates used to authenticate them; (2) seek to bind a relying party to terms of use, substantially more specific than those of local law, via a Certificate Policy ("CP") and/or Certification Practices Statement ("CPS") typically posted on a web site pointed to by a URL

embedded in the certificate, which a relying party is deemed to have accepted in virtue of the fact of reliance upon the certificate, in a manner analogous to “shrink-wrap licenses” in the world of software; and (3) rely upon methods of certificate validation that can be performed by any member of the public. Such open systems rely in part on public, local law, and in part on the presumed enforceability of the CP or CPS against the relying party, who is not in fact contractually bound to them.

The IdenTrust System is a closed contractual system, in which every subscriber and relying party is bound to a customer agreement which contractually specifies the rules under which digital signatures are agreed to be made and relied upon and the digital certificates are agreed to be valid. Local, external, public law, such as that governing sovereign recognition of digital signatures and digital certificates in any particular jurisdiction is viewed as irrelevant to the closed contractual system, so long as the customer agreements are locally enforceable, which is determined through legal analysis when the certificates are to be offered in a new jurisdiction. The certificate architecture of the system reinforces its contractual structure: a person seeking to rely upon a certificate issued within the system can do so only after receiving a positive response to a certificate validation request the party seeking to rely has digitally signed with a private key he possesses solely in virtue of being bound to a customer agreement with a Participant.

The IdenTrust System is a hierarchic PKI in which the IdenTrust Root CA licenses uniform policies, procedures, and technological specifications to its Participant financial institutions, binds them to uniform rules, and requires that their customer agreements contain uniform terms. The IdenTrust Root CA issues certificates to its participant financial institutions (each a “Participant”), whose Sub-CAs of the Root, in turn issue end entity certificates to individual certificate holders employed by customers of the Participants. Because of the uniformity of the rules and procedures throughout the system, every certificate issued by the Sub-CA of any Participant is as reliable and trustworthy as any other certificate issued by the Sub-CA of any other Participant, even if the Participants or the customers are in different countries governed by different laws.

However, local customers often want to possess, or to rely upon, certificates issued under some local policy regime. For example, certificates that are “Qualified” under the law of a European country that complies with the EU Digital Signature Directive are often commercially preferred for certain purposes in such a country. Often such certificates can be validated via a method open to the public, such as via reference to a Certificate Revocation

List generated by the CA and posted on its web site or accessible through a distribution point identified in the certificates. Accordingly, it is advantageous to the CA to be able to issue certificates that can be used both within the contractual, global system, such as the IdenTrust System, and outside it under applicable local law. Such dual use is both internal to the closed IdenTrust System at one moment of reliance and "External Use" under the alternate trust domain at another moment of reliance.

Certificates to be used for a specific purpose are typically issued within a designated trust domain. In one deployment, for example, certificates issued to certain government employees were required to be issued under the Certificate Policy applicable to that trust domain. Use of the invention permitted the issuance to said employees of IdenTrust certificates each such person could use for dual purposes, such as both access to government buildings and for electronic banking.

The operation of a PKI, and the distribution of digital credentials, readers and associated software and hardware can be expensive. It is highly advantageous to a CA, and to its subscribers and relying parties, to permit its certificates to be issued from a single platform and on a single token, but used or relied upon in multiple trust domains. This spreads the cost of the infrastructure investment across all of the trust domains and the applications that may be specific to each of them.

Accordingly, a need arose to develop a method by which a given certificate could be alternately bound to more than one policy regime (or legal, regulatory, or contractual structure) in different trust domains, at the election of the relying party at the time of reliance. This method can be generalized to any alternative trust domains.

It is crucial that there never be any doubt as to which trust domain is being bound to the certificate at any given moment of reliance. Such domains often have varying rules governing liability, recourse, and dispute resolution, and ambiguity as to which rules govern reliance upon a multi-domain certificate at any moment would be fatal to interoperability of the certificate across the trust domains. The invention assures that one and only one trust domain is bound to a certificate at any given moment by requiring that the relying party, at the moment of reliance, use a certificate validation mechanism unique to that trust domain, and thereby demonstrate its choice of the associated policy regime.

An alternative means of using a certificate in multiple trust domains that has been widely deployed in the prior art is the use of a bridge. A bridge is intended to connect the silos of multiple trust domains like a causeway connecting islands. A bridge comprises a

Certificate Authority that issues “cross-certificates” to other CAs and receives corresponding cross-certificates from such CAs so that a relying party in one trust domain can rely upon a certificate issued by a CA in another. Thus, if a relying party has CA #1 as its trust anchor, and wishes to rely upon a certificate issued by CA #2, if the bridge CA has exchanged cross-certificates with CAs #1 and #2, then the relying party whose trust anchor is CA #1 can trust CA #2 as an alternate trust anchor, and vice versa. In an architecture relying upon certificate path discovery and validation, the cross-certificates permit the relying party in question to discover the certificate path between the subscriber’s certificate (issued by CA#2) and the relying party’s ultimate trust anchor, CA #1. The cross-certification process typically requires a painstaking, and therefore expensive, mapping of the certificate policies of each of the cross-certified CAs to those of the bridge CA (to determine whether they meet common standards), as well as contracts between each CA and the Bridge CA establishing certain common understandings. Problems of cross-certification can include “transitive trust,” which can extend the opportunity of reliance upon a certificate to unintended relying parties. See, e.g., Fisher, James L., Side-Effects of Cross-Certification, http://middleware.internet2.edu/pki05/proceedings/fisher-cross_cert.pdf. The invention permits a single certificate to be trusted in multiple trust domains without policy mapping or cross-certificates, and permits a closed system to remain closed, regardless of the reliance upon the same multi-domain certificates outside the closed system.

DISCLOSURE OF INVENTION

The present invention includes a public key infrastructure comprising a participant that issues digital certificates. Each digital certificate can be relied upon in at least two different trust domains. The public key infrastructure does not employ policy mapping between or among the trust domains. Furthermore, the public key infrastructure does not link any pair of trust domains via cross-certificates.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other more detailed and specific objects and features of the present invention are more fully disclosed in the following specification, reference being had to the accompanying drawings, in which:

Figure 1 is an exemplary digital certificate that can be used in the present invention.

Figure 2 is a system level diagram of a first embodiment for implementing the present invention.

Figure 3 is a system level diagram of a second embodiment for implementing the present invention.

5 Figure 4 is a system level diagram of a third embodiment for implementing the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention consists of the following elements.

- 10 • Two distinct policy regimes – Use of a certificate alternately in either of two trust domains, each with its own policy regime, such as the IdenTrust rules, on the one hand, and an alternative regime, such as a local comprehensive law governing the use of digital certificates to authenticate digital signatures in a particular jurisdiction, on the other. The alternate regime could just as well be
15 the rules of another closed system. Such regimes contain mandatory rules governing such crucial matters as the relying party's recourse, the CA's potential liability, the kinds and maximum amounts of recoverable damages, and the procedures for lodging claims and resolving disputes, as well as the procedures for identifying subscribers, the security of keys and tokens, etc.
- 20 • Two policy OIDs – Each of the two policy regimes to which the end entity certificate is alternately to be bound must be uniquely identified by a Object Identifier ("OID") that refers to one of them. For the IdenTrust regime, that includes the applicable customer agreement, all documents incorporated therein by reference, and the public law under which the agreement is
25 enforced. For the alternate regime, it may include a CP, CPS, and the public law under which digital signatures are locally enforceable and digital certificates are locally valid.
- 30 • Interoperable certificates – IdenTrust and many other PKIs use X.509 certificates, but there are many implementations of such certificate profiles. The respective end entity certificate profiles required by the two trust domains must be such that a certificate implementing both profiles is truly interoperable in either domain, meaning that certificate processing by an application or validation utility will not fail for either of the two validation mechanisms used

for the same certificate. Where processed certificate fields that conventionally contain only one data element, such as a policy Object Identifier (“OID”) or an Authority Information Access (“AIA”) extension, contain two such elements to permit alternative certificate processing capabilities, care must be taken to test the certificates and configure the certificate processing software to permit processing of all required alternative elements without failure.

- Two Distinct validation mechanisms – When a given certificate can be validated by two distinct methods, the certificate processing software must be directed by the relying party uniquely to choose only one such method for certificate validation processing for a particular event of reliance. The key is that validation through either mechanism must be possible, but in any particular case, only one of them is selected and used. For example, a given multi-domain certificate may be validated via a signed validation request made via the Online Certificate Status Protocol (“OCSP”), or alternately by reference to a publicly posted Certificate Revocation List (“CRL”) issued by the CA. Use of different validation mechanisms for each trust domain assures that success in certificate processing will have resulted from a choice made by the relying party at the time of reliance as to which certificate validation method to employ. The relying party’s choice of certificate processing method displays its choice of trust domain, and consequently, its choice of which policy regime, and which rules, to govern that event of reliance.
- Two Issuer Certificates – Each of the end entity certificates contains an Issuer name field that names the Participant whose CA issued the certificate. Each of those certificates chains to two Issuer certificates, each with the same name in the Issuer name field, that of the Participant, and each containing the same public key corresponding to the private certificate signing key used by the CA to sign the end entity certificates. One of those Issuer certificates is used within the closed IdenTrust System, and the other is used for External Use, in the alternative trust domain. Both such issuer certificates contain the same public key and are signed by the same private key.
- Two Trust Anchors – Many certificate processing methods, such as those using CRLs, rely upon processes of first discovering the certificate path between the Trust Anchor of the relying party and that of the CA that issued

the certificate to be relied upon, and then validating each of the certificates in the path. If the method of the invention is employed in a system relying upon path discovery for both policy regimes, a separate Trust Anchor is necessary for each of them.

- 5 • The risks entailed by the policy regime of the alternative trust domain must be acceptable to the CA – Simply that the CA must be willing to accept whatever risks are attendant to issuing certificates under the policy regime that is alternative to the CA’s primary trust domain. For a Participant in the closed contractual IdenTrust system, that typically means accepting the risk that the
10 relying party will not have been enforceably bound to a relying party agreement, and thus that the Participant may not be able to enforceably limit its liability to the relying party under the law applicable to the policy regime of the alternative trust domain.
- 15 • The elements outlined above mention two distinct alternative trust domains. It is theoretically possible to issue a single certificate that is interoperable in more than two trust domains. The current realities of certificate processing (including the processing of multiple OIDs and AIAs in certificate fields) and the current lack of apparent practical demand for many more than a few trust
20 domains for a single certificate, would appear to argue against seeking to turn the “two sided coin” into a game of “pin the tail on the donkey.” One goal of the IdenTrust system is to obviate such an identity “tower of Babel” by creating in the IdenTrust System a common interoperable standard for identity credentials worldwide. The present invention then permits credentials issued within that uniform, global, closed system also to be relied upon locally under
25 the local legal regime where the relying party happens to be located.

Three embodiments of this approach have been implemented to date. They are described below as a basic method, plus two variations.

30 In one embodiment of the invention, Fig. 1 is a certificate profile that has been configured to be interoperable under both the trust domain of the IdenTrust System and that applicable to a “Qualified Certificate” under the trust domain of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community

framework for electronic Signatures (“Directive on Electronic Signatures”) regulations promulgated thereunder, and national implementing legislation.

According to the method of the invention, field 2.4.1 of Fig. 1 specifies two policy
OIDs, one specifically, the other by description. The first, represented by a string of numbers,
5 is an OID that identifies the Identity Certificate Policy of an IdenTrust Participant, and it
incorporates the balance of the policy regime applicable to reliance upon that certificate
within the IdenTrust System, i.e. the applicable Customer Agreement, the external law under
which the customer agreement is enforced against the customer who relies upon it, and the
specifications governing the method required to validate the Certificate when it is relied upon
10 within the IdenTrust System (which are incorporated by reference into the Customer
Agreement.)

The remaining language in field 2.4.1, “plus any bank xyz Policy Identifiers,”
describes another OID that is inserted into the Certificate by the IdenTrust Participant whose
CA issues it, that refers to the alternate policy regime governing the certificate when it is
15 relied upon in the other trust domain, in this case, the CP and CPS of the Participant
governing its reliance outside the IdenTrust System, and applicable law and regulations of the
local country.

Following industry practice, IdenTrust requires its Participants to include in an end
entity certificate a User Notice specifying information of which potential relying parties are to
20 take note. It is represented in field 2.4.2.1, and states, “[t]his Certificate may be relied upon
only by either: (1) a Relying Customer of an IdenTrust Participant, or (2) a party bound to the
alternative policy regime specified elsewhere in this Certificate.” The first clause governs the
use of the Certificate within the IdenTrust System, the second governs its use under the
alternate policy regime, of which the reference of the phrase “elsewhere in this Certificate” is
25 the phrase “any bank xyz Policy Identifiers” in field 2.4.1.

IdenTrust specifications require that customers of Participants who wish to rely upon
an IdenTrust certificate, such as to verify a digital signature or control access to systems or
premises, shall verify the signature and validate the certificate according to IdenTrust
specifications, which include the following specific, mandatory, requirements applicable
30 when the certificates are used within the IdenTrust System:

1. The signature must be verified using the signer’s IdenTrust certificate and the
relying customer’s software conforming to proprietary IdenTrust requirements;

2. the certificate must be validated via signed messages created by the relying customer with software conforming to proprietary IdenTrust requirements and sent in encrypted form via the OCSP to the Participant with which the relying customer has contracted to obtain its own certificates (used to validate the relying customer's signatures on the validation requests); and

3. the messaging flow of the OCSP validation requests and responses is directed according to proprietary IdenTrust requirements not compliant with IETF RFC 3280.

For purposes of the disclosure represented by the present application, the essential point is that the procedures required by IdenTrust specifications governing certificate validation are both very specific and unique. They are designed to assure that a relying party must also be a customer of an IdenTrust Participant, bound to its customer agreement governing all use of the relying party's key pair, assuring that the relying party is a relying customer, not an interloper. Validation of a signer's IdenTrust certificate in the fashion required by IdenTrust rules and specifications is contractually required by the customer agreement for the signer to be bound to the signature, and validation in any other manner is not authorized use within the IdenTrust System, but may be authorized and legally effective under the alternate trust domain if the latter's requirements are met at the time of reliance.

IdenTrust requirements permit a Participant to specify the address of its OCSP responders either with a "hard coded" IP address or via an Authority Information Access "AIA" extension. See Field 2.7 et. seq. in Fig. 1. Field 2.7.1.1 specifies that the access method is to be via OCSP, and field 2.7.1.2 states its name as a URL. Together, those two fields uniquely specify the way to address an OCSP certificate validation request to the Participant's CA that issued the certificate for use within the closed IdenTrust System. The data in the fields under 2.7.2 are proprietary and not currently in use; these fields specify communications with an IdenTrust Transaction Coordinator.

Field 2.8 is the field in which a Participant wishing to permit External Use of the certificate enters the address of a distribution point for a Certificate Revocation List. This CRL is used to validate the certificate by a relying party wishing to rely upon the certificate under the alternative policy regime of the other trust domain, in this case, the CP and CPS of the Participant governing its reliance outside the IdenTrust System, and applicable law and regulations of the local country.

It is important to note that IdenTrust rules prohibit the use of CRL distribution points in certificates intended to be used solely within the IdenTrust System, as such certificates are

permitted to be validated only via signed OCSP, to prevent parties who lack IdenTrust key pairs tied to an IdenTrust customer agreement from obtaining their validation status.

The two certificate validation mechanisms discussed above represent the choice to be made by the relying party at the moment of reliance. In this embodiment, if validation is made via signed OCSP to an AIA extension specified as required under IdenTrust rules, the certificate is bound at that moment to the policy regime of the IdenTrust trust domain. If validation is made via reference to a public CRL, and via conventional path discovery and validation, the certificate is at that moment bound to the policy regime of the alternative trust domain.

It is critical that a certificate to be alternately bound to two different trust domains can successfully validate in each of them. To assure that validation in the alternate domain is successful, all of the elements and steps required for successful validation within that domain must be possible. Thus, for example, in a trust domain that requires certificate path discovery to an external trust anchor, and path validation to a CRL it has posted, an external trust anchor will be necessary to serve as the terminus of the validation path or validation will fail.

1st Embodiment: Self-Signed Issuer Certificate. (Figure 2) A Participant's CA possesses a certificate signing private key that corresponds to a public key. In the standard deployment within the IdenTrust System, the IdenTrust Root CA issues Issuer certificates containing that public key of the Participant, and naming the Participant in its subject name fields. When the Participant's CA issues end entity certificates, those certificates name the Participant in their Issuer name fields and the Subscriber in their subject name fields. (See fields 1.4.2 and 1.6.2 in Fig. 1, respectively). The trust anchor for such certificates is the IdenTrust Root CA certificate. As discussed above, a party wishing to rely upon such an end entity certificate within the IdenTrust System must be a customer of an IdenTrust Participant, who possesses a key pair solely in virtue of being bound to an IdenTrust customer agreement with that Participant, and who must use its private key to sign, and its own end entity certificate to authenticate, the certificate status request it must send to its Participant via signed OCSP to validate the certificate of the subscriber.

In the first embodiment, when an end entity certificate issued to an IdenTrust subscriber is also to be used outside the IdenTrust System, for External Use, the CA of the Participant issues a second, "self-signed" Issuer certificate to itself, naming the Participant in both the Issuer and subject name fields, and containing the same public key that is contained in the Issuer certificate described in the preceding paragraph. An end entity certificate signed

by the Participant's private certificate signing key can be verified by the public key in both Issuer certificates. If a party wishes to rely upon the end entity certificate is an IdenTrust customer, it will validate the certificate in the manner described in the preceding paragraph. If a party wishes to rely upon the end entity certificate through External Use under an alternative policy regime, such as one provided under local law, it may validate the certificate via conventional path discovery and validation. In such a case, the self-signed Issuer certificate serves as the Trust Anchor, and the relying party can determine the validity of the subscriber's end entity certificate by reference to a public CRL issued by the Participant's CA, such as by reference to a CRL Distribution Point specified in field 2.8 of Fig. 1.

The Participant's IdenTrust Customer Agreement requires that if the relying party wishes to use the certificate within the IdenTrust System, and therefore to bind the certificate at any given moment of reliance to the Participant's IdenTrust policy regime, it must validate the certificate in the manner required by that agreement, i.e. via signed OCSP validation request. For External Use of the certificate, the applicable policy regime, such as that specified in a CPS published by the Participant governing such use, will specify what method(s) of validation are permissible. Accordingly, the election by the relying party of the method of validation of the certificate demonstrates its choice of which policy regime to bind to the certificate at a given moment of reliance. If the relying party is a customer of an IdenTrust Participant, it is therefore potentially capable of either means of validating the same certificate, and its choice will demonstrate whether the certificate is governed at that moment under IdenTrust global rules, or local law.

2nd Embodiment: A Second Root CA Certificate. (Fig. 3) In another embodiment, the alternate trust domain may be hierarchic, and may have its own Root CA. In such a case, the Participant obtains the signature of the other Root CA upon a certificate containing the public key corresponding to the Participant's certificate signing private key. In such a fashion, path discovery and validation during External Use will proceed to the trust anchor of that alternate trust domain, in this case, to its Root CA. In other words, in such a deployment, the Participant operates a CA that is both a Sub-CA of the IdenTrust Root CA and a Sub-CA of the other Root CA, which share a common key pair for signing and validating subscriber certificates. The two Sub-CAs can be configured to share substantial portions of their infrastructure, thereby substantially reducing the cost of operating both.

3rd Embodiment: Connection to a Bridge. (Fig. 4) In yet another embodiment, the alternate trust domain may be connected to a bridge. Briefly, a bridge CA exchanges cross-

certificates with other CAs so that subscribers within one trust domain can rely upon certificates issued within others. In this third embodiment, the Participant's private key signs a cross-certificate issued to the bridge that can be validated against the self-signed Issuer certificate of the alternate trust domain. If desired, the bridge may also issue a cross-certificate to the Participant permitting the Participant's subscribers also to rely upon certificates issued by other CAs connected to it via the bridge.

The method of this invention can be generalized to any other method of certificate validation. A matrix of possible variations could be constructed, for example:

- Signed v. unsigned OCSP
- Whether the OCSP communication is made via a secure SSL session or not (https v. http)
- In the case of SSL, whether the certificate used is low security or high security (such as an IdenTrust Utility Certificate, issued by the CA of a Participant that chains to the IdenTrust Root CA)
- OCSP to different addresses (whether hard coded IP addresses, URL AIAs, or a single AIA with multiple locations)
- OCSP v. SCVP ("Simple Certificate Validation Protocol") (or any other protocol)
- Validation that complies with RFC 3280, and that which does not
- OCSP v. path discovery and validation
- Almost anything other than path discovery and validation under RFC 3280 to different trust anchors (which would follow two inconsistent validation paths therefore presumably fail to demonstrate actual relying party choice between validation methods).

In addition, the method can be further generalized to any means of distinguishing two trust domains. It need not be limited to distinguishing between trust domains by reference to policy identifiers and validation mechanisms. One could establish by rule or contract that a given Issuer could have alternative issuer names in any of one or more specified fields, or could contain a field, the presence of which creates an alternative certificate processing path, associated with an alternative policy regime.

Finally, as noted earlier, the alternative trust domains linked by a single end entity certificate need not be limited to two. There is no limit to the number of trust domains in

which a given end entity certificate can be relied upon. The only limit is whether available certificate processing software will reliably process all the variations.

The above description is included to illustrate the operation of the preferred embodiments, and is not meant to limit the scope of the invention. The scope of the invention is to be limited only by the following claims. From the above discussion, many variations will be apparent to one skilled in the art that would yet be encompassed by the spirit and scope of the present invention.

What is claimed is:

CLAIMS

1. A public key infrastructure comprising a participant that issues a digital certificate,
wherein the digital certificate can be relied upon in at least two different trust domains,
5 wherein:

said public key infrastructure does not employ policy mapping between or among the
trust domains; and

said public key infrastructure does not link any pair of trust domains via cross-
certificates.

10 2. The public key infrastructure of claim 1 wherein at least one trust domain is a
closed contractual domain.

3. The public key infrastructure of claim 1 wherein at least one trust domain is an
open trust domain.

15 4. The public key infrastructure of claim 3 wherein the digital certificate is qualified
under the law of a European country that complies with the European Digital Signature
Directive.

5. The public key infrastructure of claim 1 wherein just one trust domain is bound to
the digital certificate at any given moment.

20 6. The public key infrastructure of claim 1 wherein the digital certificate is relied
upon by a relying party; and

the current trust domain that is to be bound to the digital certificate is elected by the
relying party at the time of reliance, based upon a specific certificate validation methodology
selected by the relying party.

25 7. The public key infrastructure of claim 6 wherein the certificate validation
methodology is a methodology from the group of methodologies consisting of:

a signed validation request made via an Online Certificate Status Protocol; and
making reference to a publicly posted Certificate Revocation List issued by the
participant.

8. The public key infrastructure of claim 1 wherein different trust domains have different rules governing liability, recourse, and dispute resolution.

9. The public key infrastructure of claim 1 wherein each trust domain comprises a policy that is uniquely identified by an Object Identifier.

5 10. The public key infrastructure of claim 9 wherein each Object Identifier comprises at least one of:

 a customer agreement;

 documents incorporated by reference in a customer agreement;

 public law under which a policy is enforced;

10 a Certificate Policy;

 a Certification Practices Statement;

 public law under which digital signatures are locally enforceable and digital certificates are locally valid.

15 11. The public key infrastructure of claim 1 wherein a first trust domain is trust anchored by a root digital certificate issued to the participant, and a second trust domain is trust anchored by a digital certificate self-signed by a certificate authority of the participant.

20 12. The public key infrastructure of claim 1 wherein a first trust domain is trust anchored by a first digital certificate that is issued to the participant by a first root certificate authority, and a second trust domain is trust anchored by a second digital certificate that is issued to the participant by a second root certification authority.

25 13. The public key infrastructure of claim 1 wherein a first trust domain is trust anchored by a first digital certificate issued to the participant by a first root certificate authority, and a second trust domain is trust anchored by a second digital certificate that is coupled to the participant by a bridge certification authority digital certificate.

1/6

End-Entity Qualified Business Identity Hardware Certificate Profile

Field	Content	Mandatory	Critical
1. X.509v1 Field			
1.1. Version	v3	y	
1.2. Serial Number	Allocated automatically by the Issuing CA	y	
1.3. Signature Algorithm	SHA-1 with RSA Signature	y	
1.4. Issuer Distinguished Name		y	
1.4.1. Country (C)	Not Required	n	
1.4.2. Organization (O)	e.g., "Bank XYZ"	y	
1.4.3. Organizational Unit (OU)	e.g., "Bank XYZ Identrus Authority"	y	
1.4.4. Common Name (CN)	e.g., "Bank XYZ Identrus Authority"	y	
1.5. Validity		y	
1.5.1. Not Before	e.g., "00:00:01 01 September 1999"	y	
1.5.2. Not After	e.g., "23:59:59 31 August 2003"	y	
1.6. Subject		y	
1.6.1. Country (C)	Required	y	
1.6.2. Organization (O)	e.g., "The XYZ Company"	y	
1.6.3. Organizational Unit (OU)	e.g., "International Financial Services"	y	
1.6.4. Common Name (CN)	e.g., "John Doe"	y	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC 3280 & PKCS#1	y	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		y	n
2.1.1. Key Identifier	the Subject Key Identifier of the Issuer of this Certificate	y	
2.1.2. AuthorityCertIssuer	Not present	n	
2.1.3. AuthorityCertSerialNumber	Not present	n	

FIG. 1A

2/6

Field	Content	Mandatory	Critical
2.2. Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	y	n
2.3. Key Usage		y	Y
2.3.1. Digital Signature	Not selected "0"	y	
2.3.2. Non Repudiation	Selected "1"	y	
2.3.3. Key Encipherment	Not selected "0"	y	
2.3.4. Data Encipherment	Not selected "0"	y	
2.3.5. Key Agreement	Not selected "0"	y	
2.3.6. Key Certificate Signature	Not selected "0"	y	
2.3.7. CRL Signature	Not selected "0"	y	
2.4. Certificate Policies		y	n
2.4.1. Policy Identifier	1.2.840.114021.1.30.2 plus any BankXYZ Policy Identifiers	y	
2.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	y	
2.4.2.1. User Notice	This Certificate may be relied upon only by either: (1) a Relying Customer of an Identrus Participant, or (2) a party bound to the alternative policy regime specified elsewhere in this Certificate	y	
2.4.2.2. Policy Identifier	Optional Policy Identifiers to be defined by Participant	n	
2.4.2.3. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	n	
2.4.2.4. User Notice	Optional to be defined by Participant	n	
2.5. Subject Alternate Names	Optional	n	n
2.5.1. rfc822Name	e.g., "john.doe@XYZCorp.com"	y	
2.5.2. registeredID	Optional, "OID as per IP-NAMOID"	n	
2.6. Basic Constraints	Not present	n	
2.6.1. Subject Type	Not present	n	
2.6.2. Path Length Constraint	Not present	n	

FIG. 1B

3/6

Field	Content	Mandatory	Critical
2.7. Authority Information Access		y	N
2.7.1. Access Description		y	
2.7.1.1. Access Method	On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1)	y	
2.7.1.2. Alternative Name	e.g., "URL=https://IV.OCSP.Bank-XYZ.com"	y	
2.7.2. Access Description			
2.7.2.1. Access Method	IdenTrust Certificate Status Check Protocol(1.2.840.114021.4.1)	y	
2.7.2.2. Alternative Name	"URL=https://xyz.abcBank.com"	y	
2.8. CRLDistributionPoint		n	
2.9. QC Statements		n	n

FIG. 1C

1st Embodiment – Self Signed Certificate

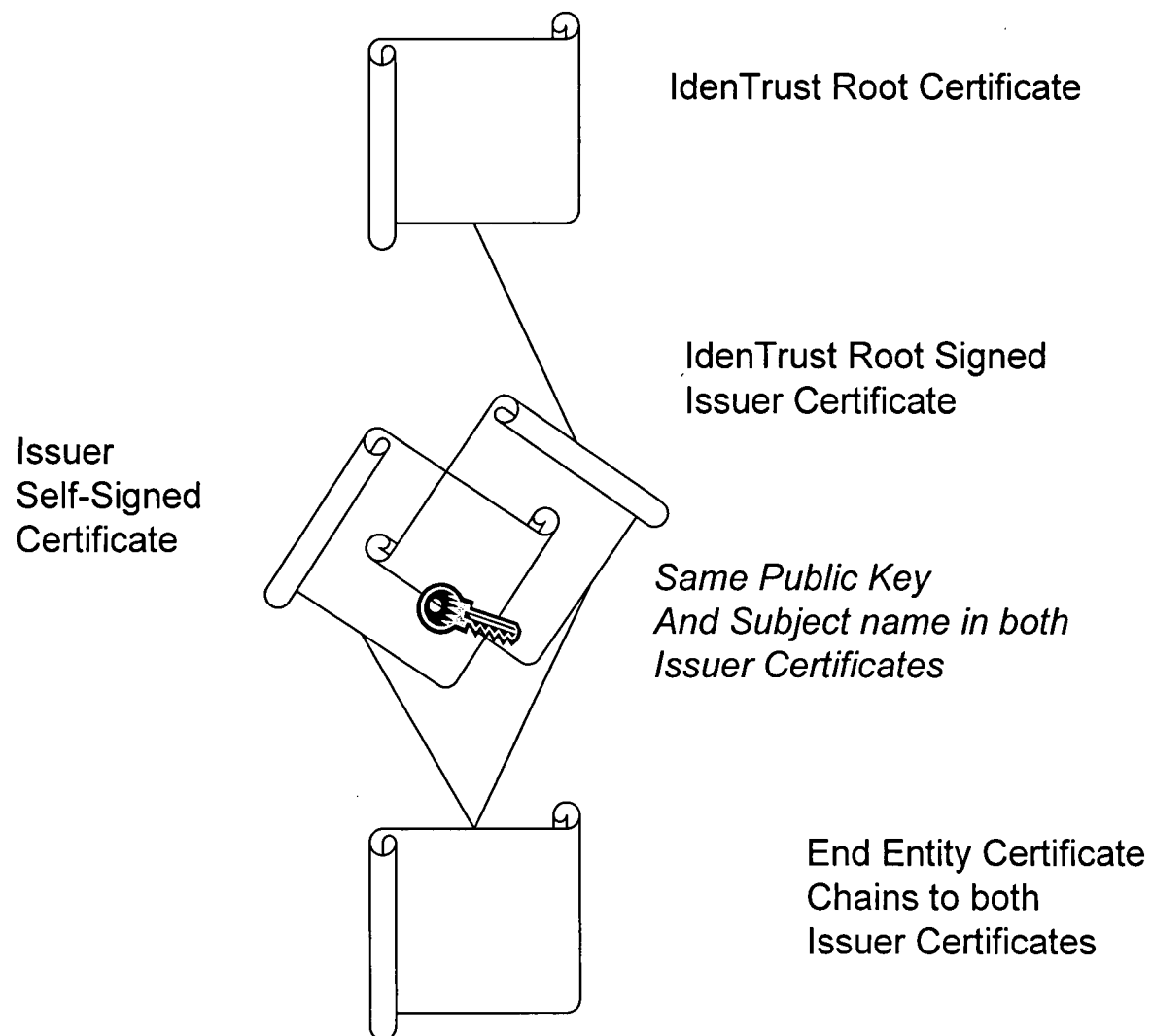
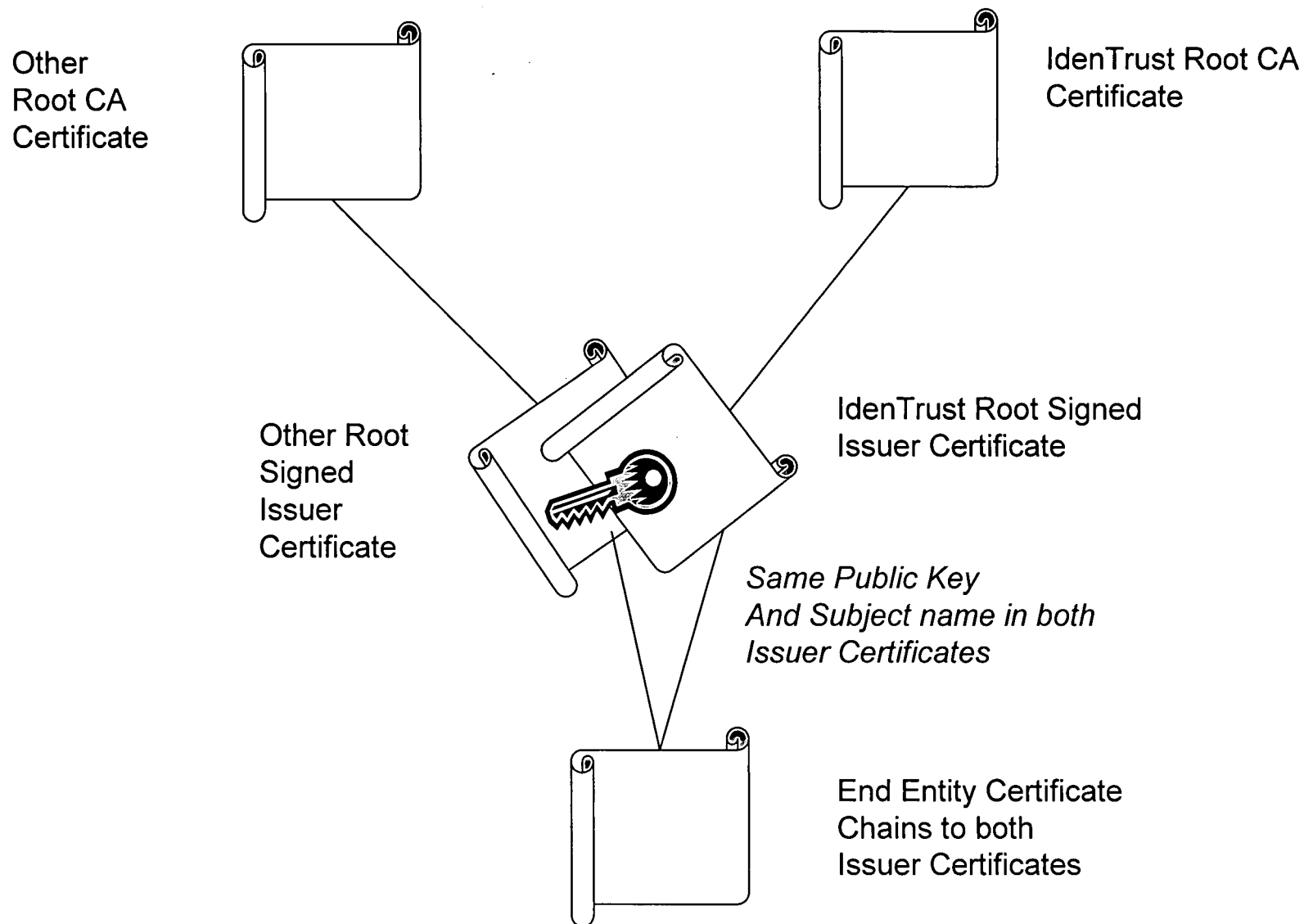


FIG. 2

5/6

2nd Embodiment – A Second Root CA

**FIG. 3**

3rd Embodiment – Connection to a Bridge

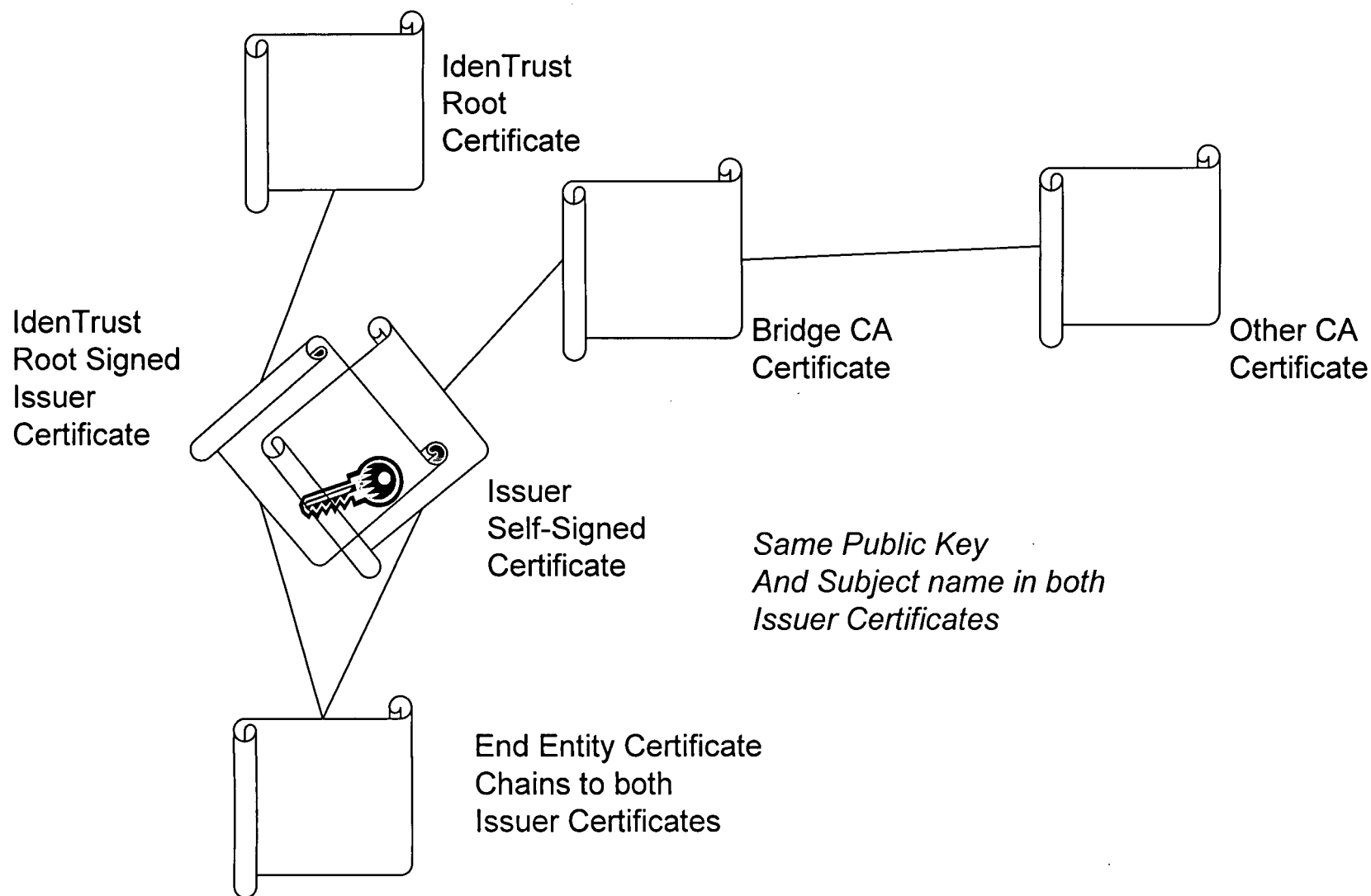


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 09/00357

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/00 (2009.01)

USPC - 713/156

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)

IPC (8) - H04L 9/00 (2009.01)

USPC - 713/156

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

USPC - 713/150, 155, 156, 182 (See Keywords Below)

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

Pub WEST (USPT, PGPB, JPAB, EPAB), Google Scholar

Search Terms Used: public key infrastructure, PKI, digital certificate, trust domain, policy map, cross-certificate, pair of domain, European Digital Signature Directive, status protocol, validating certificate, revocation list, customer agreement, root certificate,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0187031 A1 (LIDDLE), 23 September 2004 (23.09.2004), entire document, especially Abstract; para [0015]-[0018]; [0064]-[0066]; [0078]-[0079] and [0110]-[0112]	1-13
Y	US 2005/0132229 A1 (ZHANG et al.), 16 June 2005 (16.06.2005), entire document, especially para [0024]-[0028]; [0060]-[0062]; [0073]-[0074] and [0080]-[0081]	1-13
Y	US 2008/0010665 A1 (HINTON et al.), 10 January 2008 (10.01.2008), entire document, especially para [0094]-[0095]	2-4
Y	US 2002/0065695 A1 (FRANCOEUR et al.), 30 May 2002 (30.05.2002), entire document, especially para [0104] and [0126]-[0128]	4, 7 and 9-10



Further documents are listed in the continuation of Box C.



* 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

11 March 2009 (11.03.2009)

Date of mailing of the international search report

24 MAR 2009

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774