US 20100115266A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2010/0115266 A1**

GUO et al. (43) **Pub. Date: May 6, 2010**

(54) **METHOD AND DEVICE FOR ENABLING A TRUST RELATIONSHIP USING AN UNEXPIRED PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE**

(75) Inventors: **Liang GUO**, Brighton, MA (US); **Whay Chiou Lee**, Cambridge, MA (US); **Anthony R. Metke**, Naperville, IL (US)

Correspondence Address:
MOTOROLA, INC
1303 EAST ALGONQUIN ROAD, IL01/3RD
SCHAUMBURG, IL 60196 (US)

(73) Assignee: **MOTOROLA, INC.**, Schaumburg, IL (US)

(21) Appl. No.: **12/262,761**

(22) Filed: **Oct. 31, 2008**

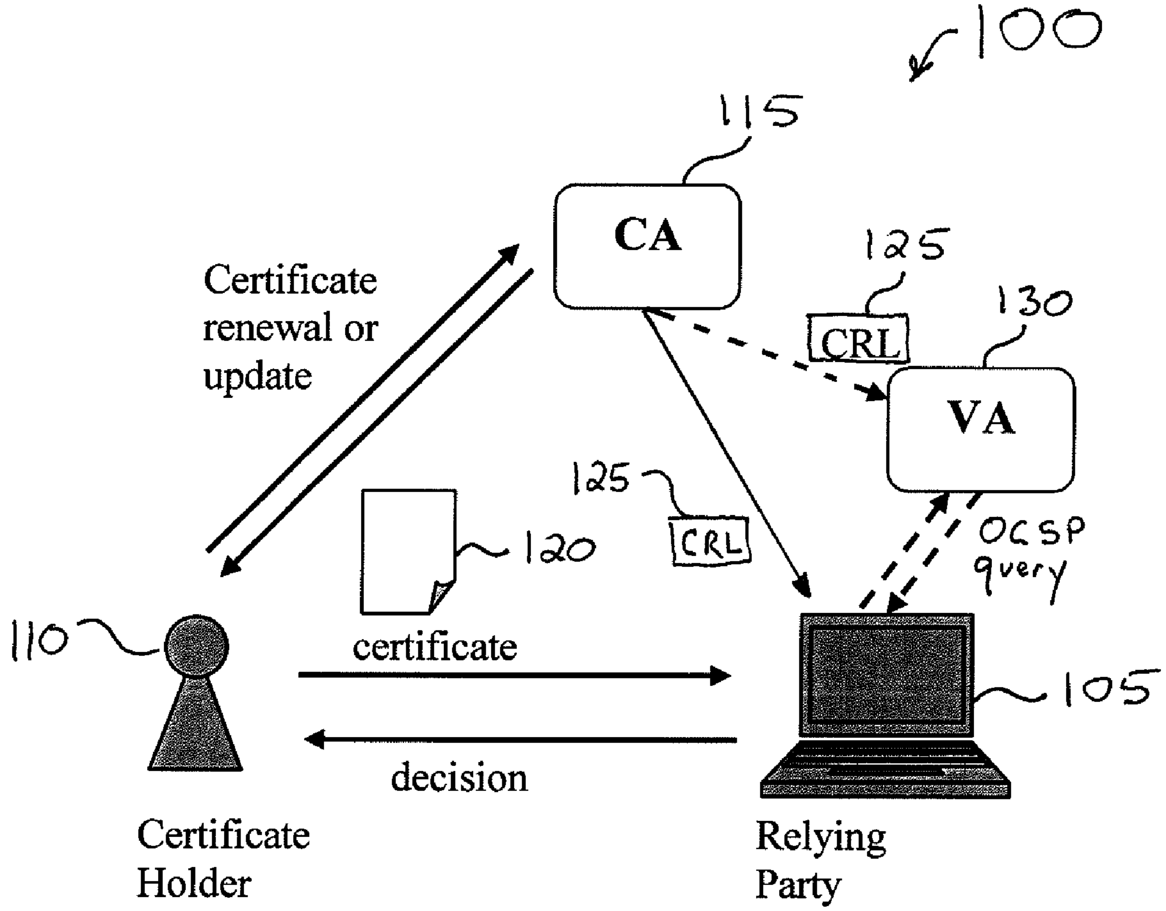
Publication Classification

(51) **Int. Cl.**
H04L 9/06 (2006.01)

(52) **U.S. Cl.** **713/156**

(57) **ABSTRACT**

A method and device are useful for enabling a trust relationship using an unexpired public key infrastructure (PKI) certificate, where a current status of the PKI certificate is unavailable. The method includes determining at a relying party that a certificate status update for the PKI certificate is unavailable (step **905**). Next, in response to the certificate status update being unavailable, a tolerable certificate status age (TCSA) for the PKI certificate is determined at the relying party based on one or more attributes associated with a certificate holder of the PKI certificate (step **910**). Using the PKI certificate, a trust relationship is enabled between the relying party and the certificate holder after determining the TCSA and before an expiration of the TCSA (step **915**).



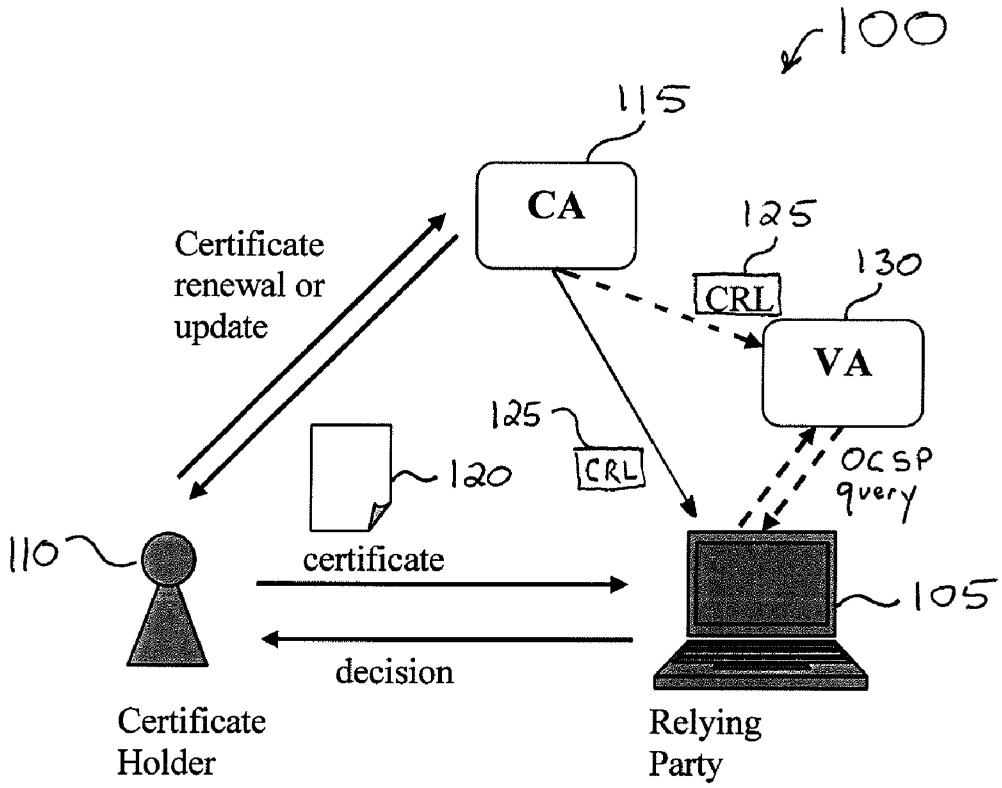

100
115
CA
125
CRL
130
VA
Certificate renewal or update
125
CRL
120
OCSP query
110
certificate
105
decision
Certificate Holder
Relying Party

FIG. 1

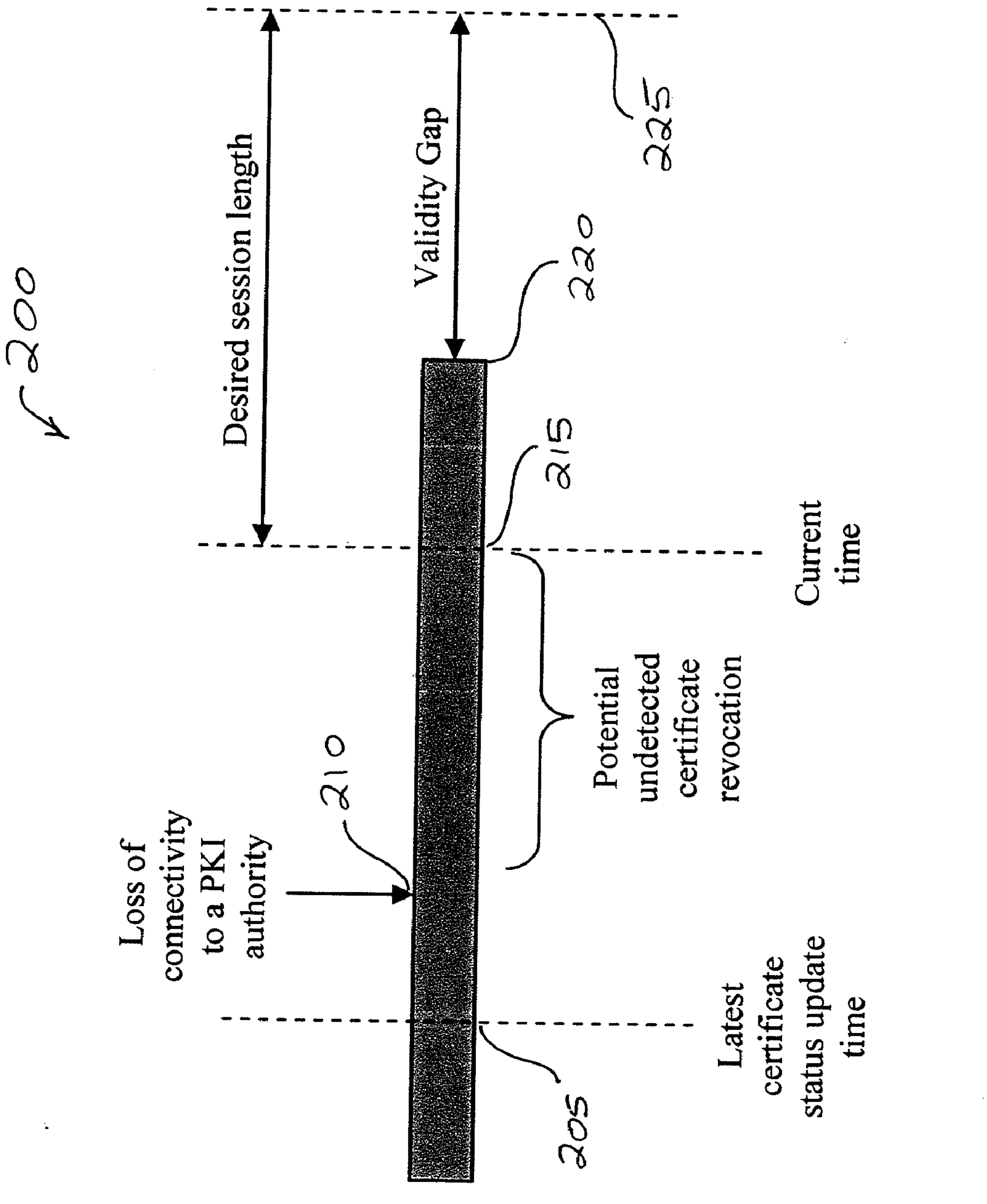

200
Desired session length
Validity Gap
225
220
215
Current time
Potential undetected certificate revocation
210
Loss of connectivity to a PKI authority
Latest certificate status update time
205

FIG. 2

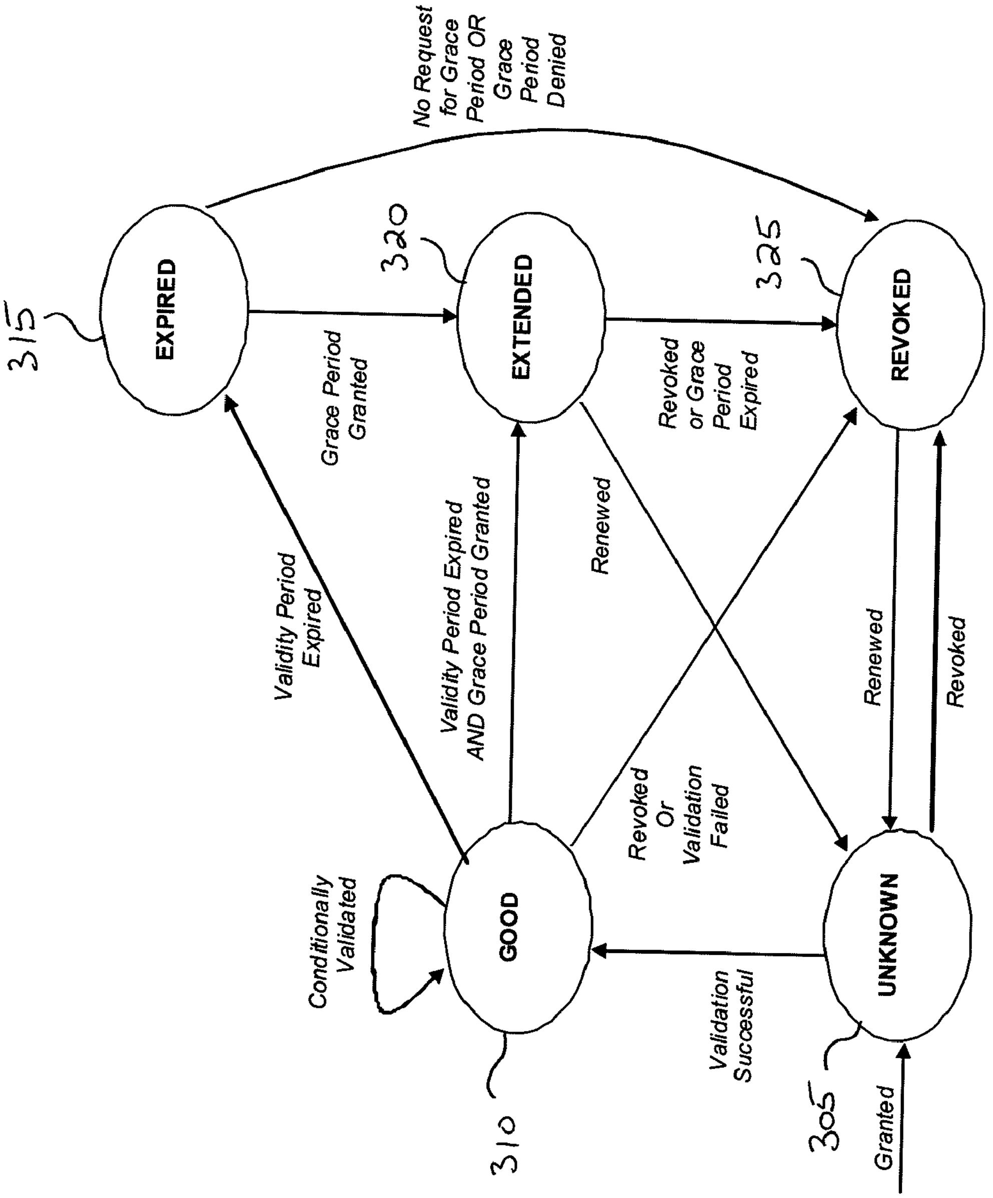

EXPIRED
315
EXTENDED
320
REVOKED
325
GOOD
310
UNKNOWN
305
No Request for Grace Period OR Grace Period Denied
Grace Period Granted
Revoked or Grace Period Expired
Validity Period Expired
Validity Period Expired AND Grace Period Granted
Renewed
Revoked Or Validation Failed
Renewed
Revoked
Conditionally Validated
Validation Successful
Granted

FIG. 3

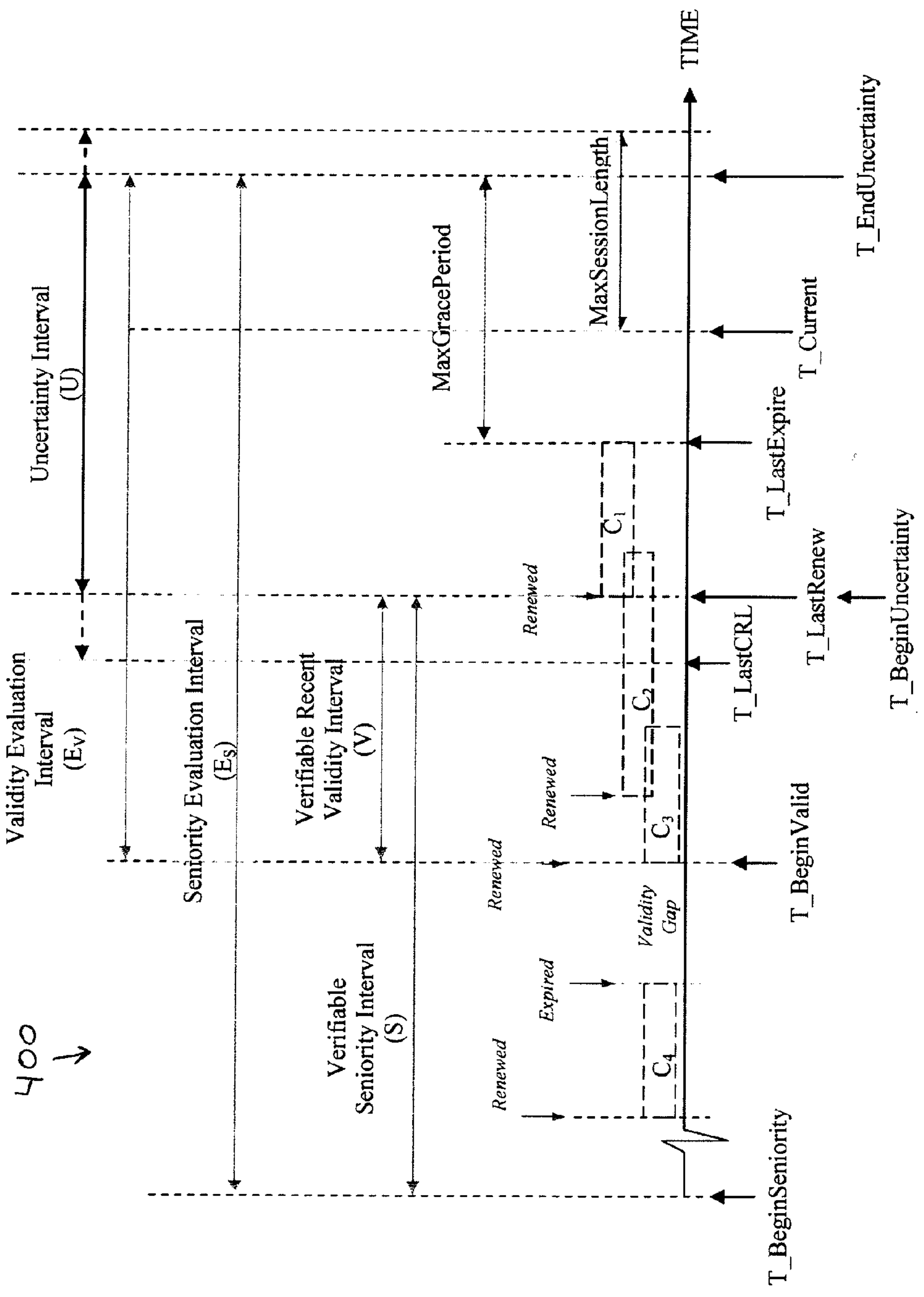

400
TIME
T_EndUncertainty
T_Current
T_LastExpire
T_LastRenew
T_BeginUncertainty
T_LastCRL
T_BeginValid
T_BeginSeniority
Uncertainty Interval (U)
MaxGracePeriod
MaxSessionLength
Validity Evaluation Interval (E_V)
Seniority Evaluation Interval (E_S)
Verifiable Recent Validity Interval (V)
Verifiable Seniority Interval (S)
C1
C2
C3
C4
Renewed
Renewed
Renewed
Expired
Renewed
Validity Gap

FIG. 4

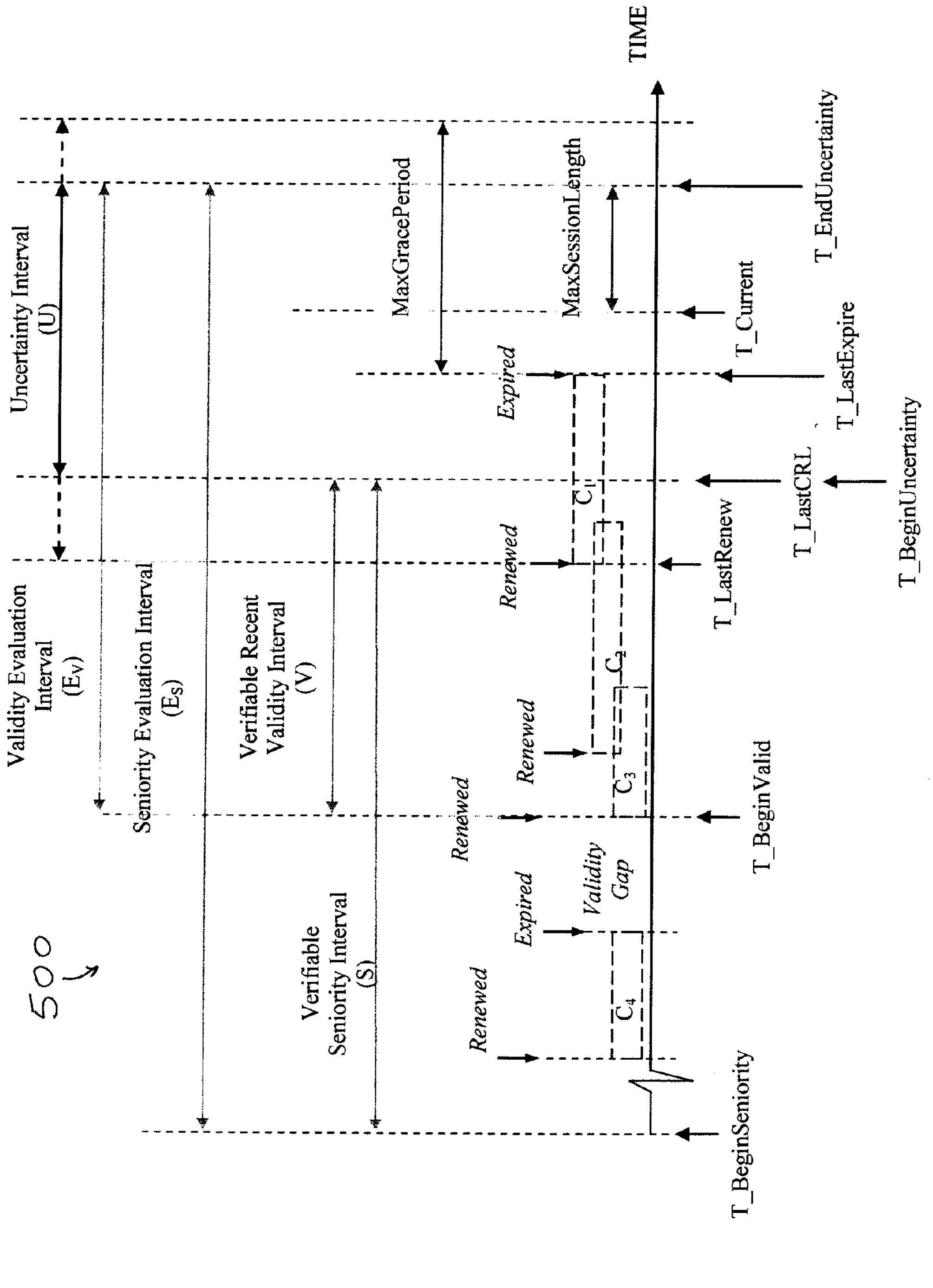

500
TIME
Uncertainty Interval
(U)
Validity Evaluation
Interval
(E_V)
Seniority Evaluation Interval
(E_S)
Verifiable Recent
Validity Interval
(V)
Verifiable
Seniority Interval
(S)
MaxGracePeriod
MaxSessionLength
Expired
Renewed
Renewed
Renewed
Expired
Renewed
Validity
Gap
C_1
C_2
C_3
C_4
T_EndUncertainty
T_Current
T_LastExpire
T_LastCRL
T_BeginUncertainty
T_LastRenew
T_BeginValid
T_BeginSeniority

FIG. 5

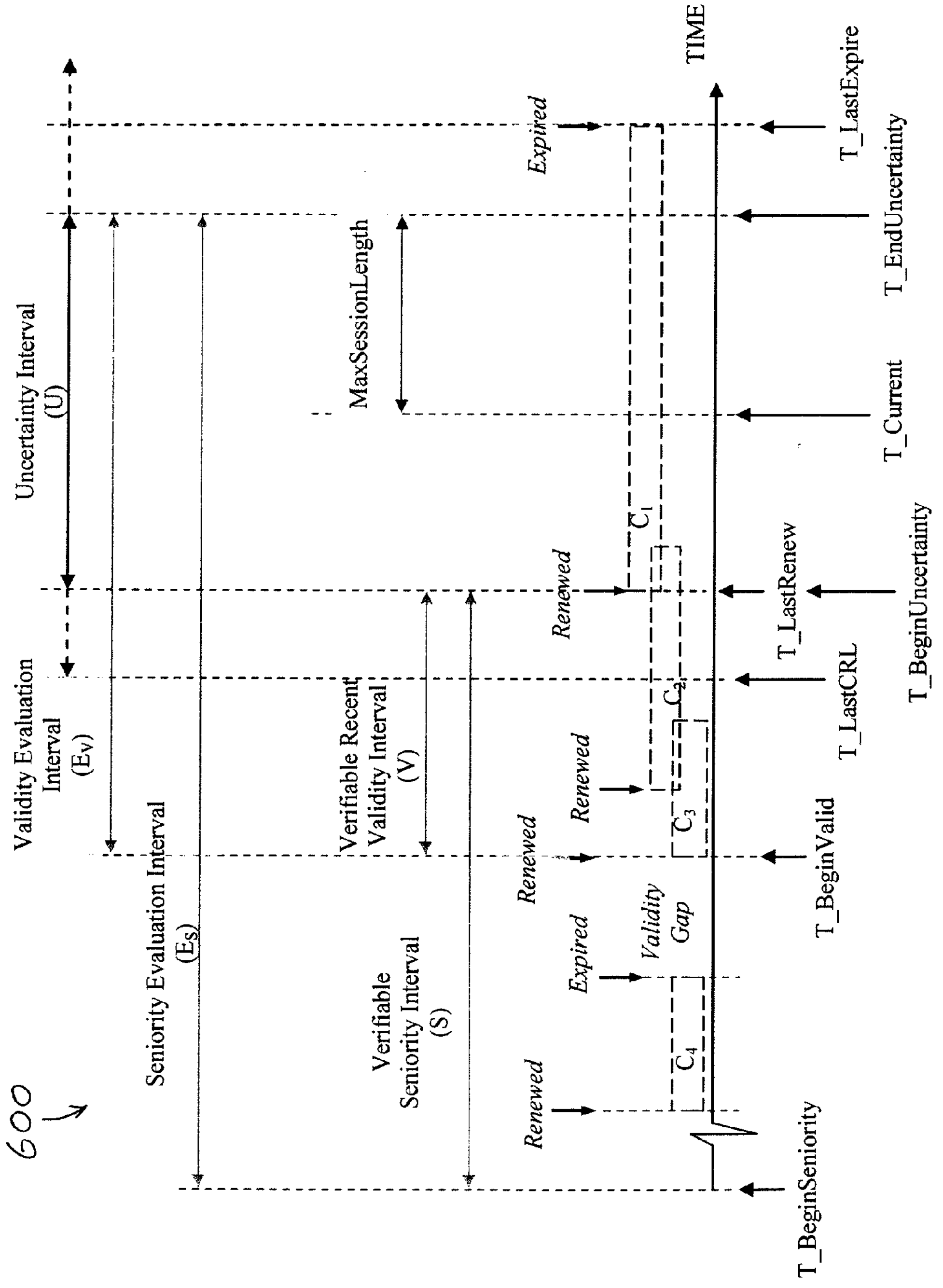

600
Validity Evaluation Interval (EV)
Uncertainty Interval (U)
Seniority Evaluation Interval (ES)
Verifiable Recent Validity Interval (V)
MaxSessionLength
Verifiable Seniority Interval (S)
Renewed
Expired
Validity Gap
Renewed
Renewed
Renewed
Expired
C1
C2
C3
C4
TIME
T_LastExpire
T_EndUncertainty
T_Current
T_BeginUncertainty
T_LastRenew
T_LastCRL
T_BeginValid
T_BeginSeniority

FIG. 6

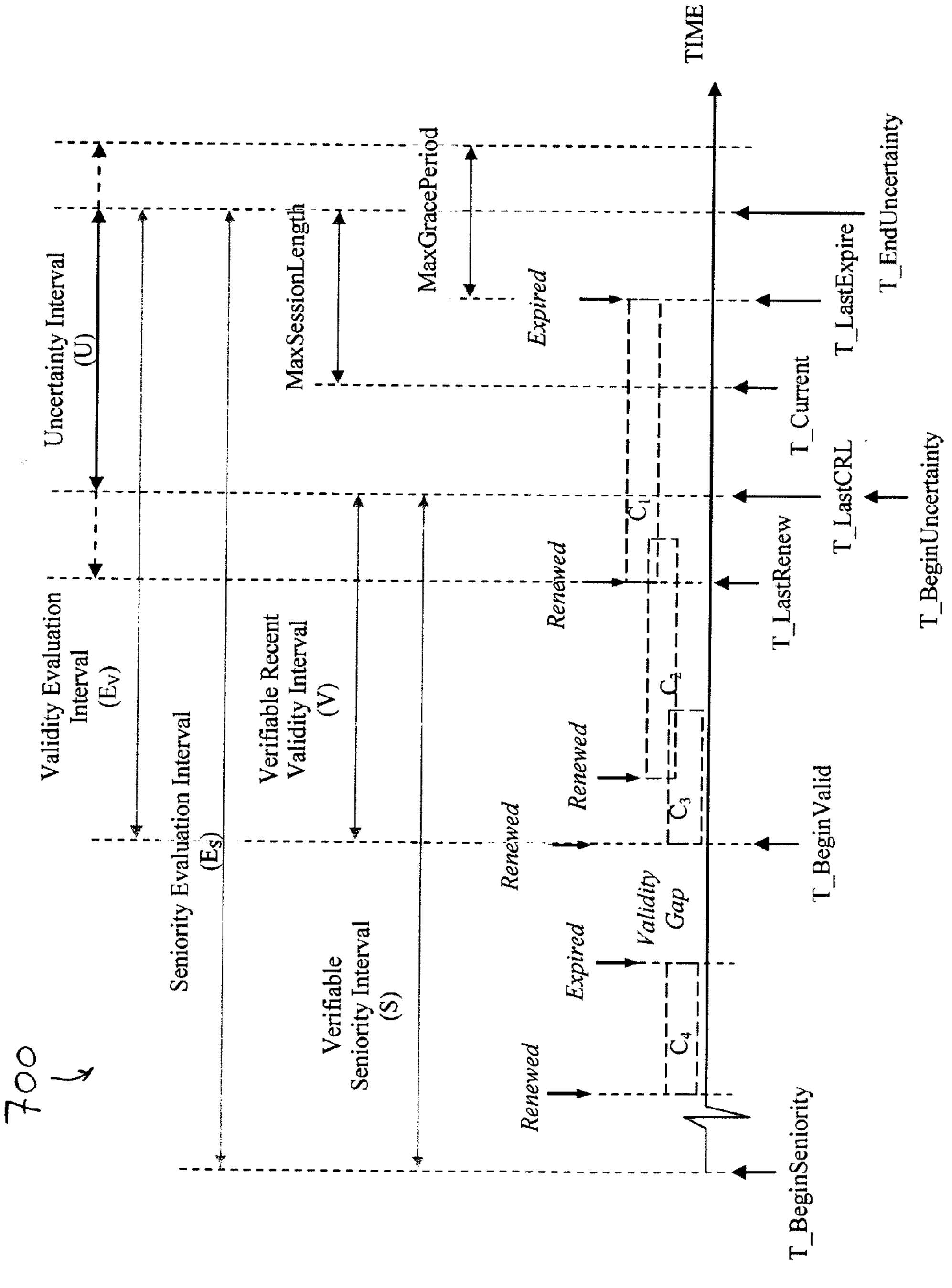

700
TIME
Uncertainty Interval
(U)
Validity Evaluation
Interval
(E_V)
Seniority Evaluation Interval
(E_S)
Verifiable Recent
Validity Interval
(V)
Verifiable
Seniority Interval
(S)
MaxSessionLength
MaxGracePeriod
Expired
Renewed
Renewed
Renewed
Validity
Gap
Expired
Renewed
C_1
C_2
C_3
C_4
T_EndUncertainty
T_LastExpire
T_Current
T_LastCRL
T_BeginUncertainty
T_LastRenew
T_BeginValid
T_BeginSeniority

FIG. 7

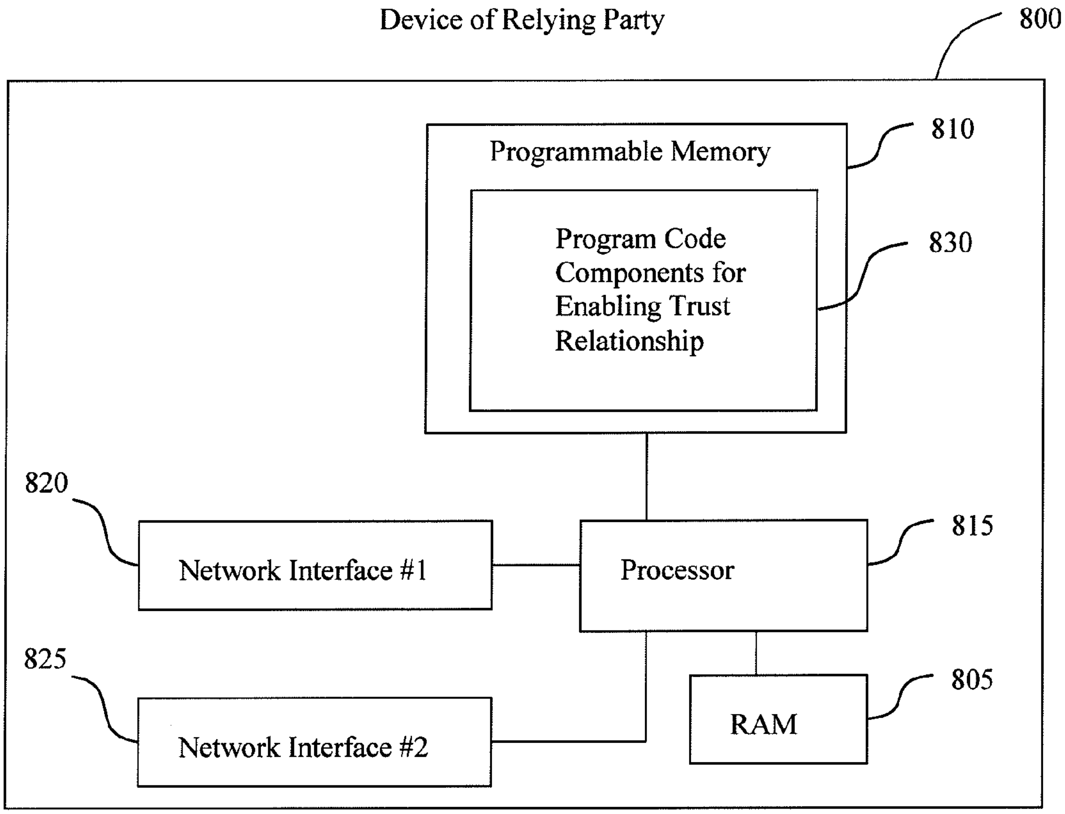

Device of Relying Party
800
Programmable Memory
810
Program Code Components for Enabling Trust Relationship
830
820
Network Interface #1
Processor
815
825
Network Interface #2
RAM
805

FIG. 8

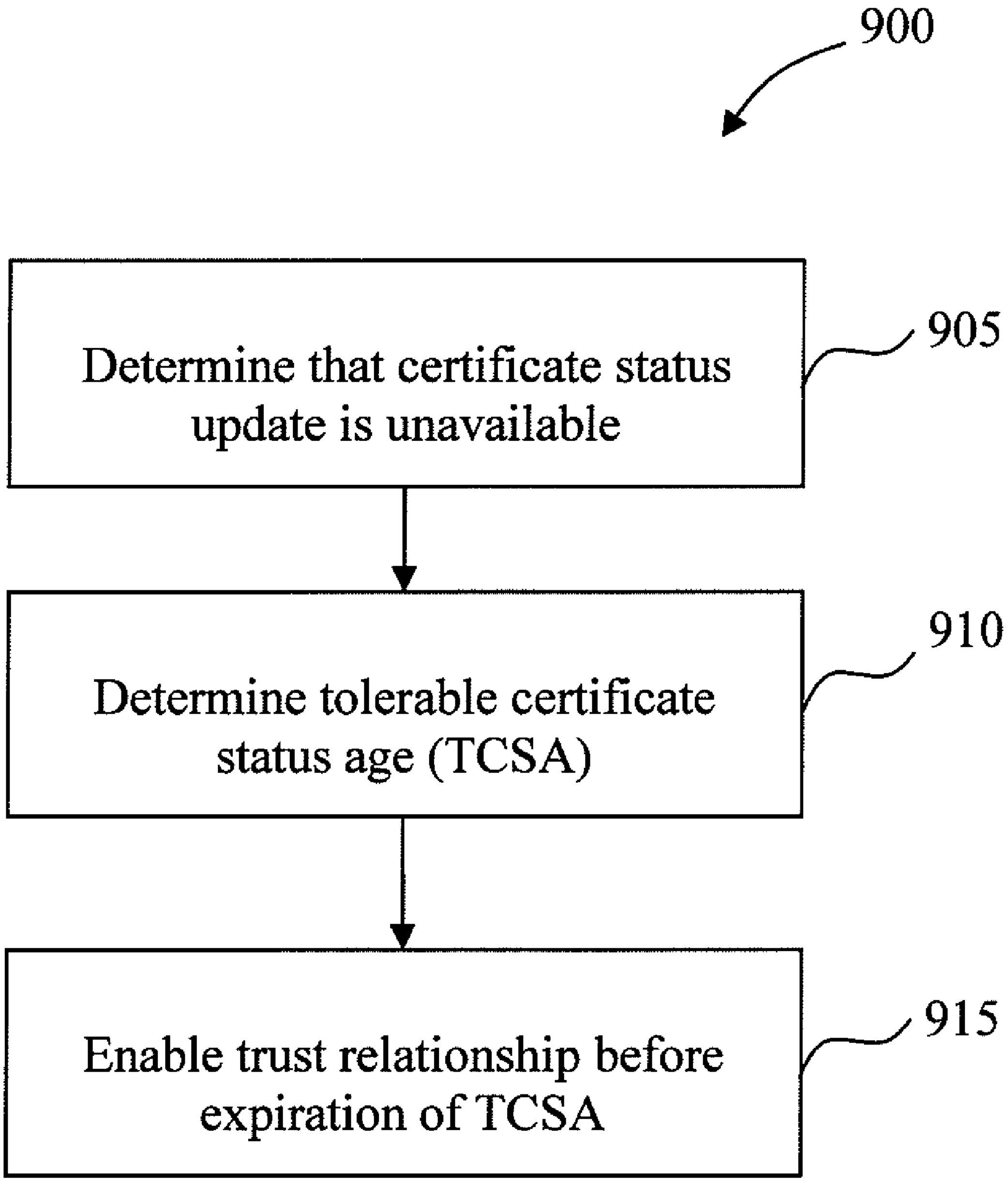

900
Determine that certificate status update is unavailable
905
Determine tolerable certificate status age (TCSA)
910
Enable trust relationship before expiration of TCSA
915

FIG. 9

METHOD AND DEVICE FOR ENABLING A TRUST RELATIONSHIP USING AN UNEXPIRED PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application is related to the following U.S. application commonly owned with this application by Motorola, Inc.: U.S. Patent Application of Liang Guo entitled "Method And Device For Enabling A Trust Relationship Using An Expired Public Key Infrastructure (PKI) Certificate", Attorney Docket Number CM12322, filed concurrently herewith, the entire contents of which being incorporated herein by reference.

FIELD OF THE DISCLOSURE

[0002] The present invention relates generally to security and trust management in communication networks, and in particular to enabling a trust relationship using an unexpired public key infrastructure (PKI) certificate where a current status of the PKI certificate is unavailable.

BACKGROUND

[0003] Security in a communication network can be enhanced through use of a public key infrastructure (PKI). A PKI provides mechanisms to bind public keys to entities, enable other entities to verify public key bindings, and provide the services needed for ongoing management of keys in a distributed system. By supporting public key based authentication, a PKI also improves confidentiality, integrity and authentication of communications. A primary function of a PKI is to provide a relying party assurance of the validity of certificates possessed by a certificate holder. The certificates are issued and signed by a third party, called a certification authority (CA), which is trusted by both the certificate holder and the relying party. Overall network security is thus often dependent on the validity, and hence trustworthiness, of individual certificates.

[0004] As all public-key schemes are at least to some degree susceptible to security attacks, such as a brute force key search attack, various PKI security precautions are generally employed. For example, each public key certificate generally has a validity period, beyond which the certificate becomes invalid (equivalently, the certificate is said to have expired). Also, a certificate may be proactively revoked by the CA that issued it, or by a certificate holder if any compromise of key security is detected.

[0005] A CA is generally responsible for advertising certificate status information of active certificates to all relying parties, either proactively through publishing certificate revocation lists (CRLs), or reactively by responding to on-demand requests (e.g., through a validation authority (VA) using an Online Certificate Status Protocol (OCSP)). With proactive publication of a CRL, each period between successive advertisements is a vulnerable interval during which revocation of a certificate may be undetectable by a relying party. With on-demand requests, certificate status update delays can be increased by the unavailability of a connection to an OCSP server, or by the inability of an OCSP server to obtain a certificate revocation status from a CA.

[0006] A certificate holder conventionally must maintain a valid certificate issued by a CA in order to continue making trustworthy transactions with relying parties that trust the CA. When a certificate approaches expiration, the certificate holder may request the CA to renew the certificate for an extended validity period, but without changing a distinguished name, attributes, or a key associated with the certificate. A certificate holder of a revoked certificate may obtain a new certificate from the CA that issued the original certificate through a certificate update process, by which the CA grants a new certificate with the same distinguished name, but with one or more updated or new attributes, a new key, a new serial number, and possibly a new validity period. Certificate renewals and certificate updates require existence of a secure communication channel between a CA and a certificate holder. Further, confirmation of certificate renewals and certificate updates may require existence of a secure communication channel between a CA and a relying party.

[0007] However, even when a secure communication channel between a CA and a certificate holder is unavailable, and/or when a secure communication channel between a CA and a relying party is unavailable, use of an unexpired PKI certificate still may be required.

BRIEF DESCRIPTION OF THE FIGURES

[0008] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed invention, and explain various principles and advantages of those embodiments.

[0009] FIG. **1** is a diagram illustrating a communication network that includes open communication channels between a relying party, a certificate holder, a validation authority (VA), and a certification authority (CA).

[0010] FIG. **2** is a certificate timeline illustrating a need for a tolerable certificate status age (TCSA) and a certificate grace period of a PKI certificate, according to some embodiments.

[0011] FIG. **3** is a certificate state diagram illustrating five possible states of a certificate, according to some embodiments.

[0012] FIG. **4** is timeline illustrating defined variables and intervals in circumstances where a most recent certificate was renewed after a last certificate revocation list (CRL) update was received, and the certificate expired before the current time, according to some embodiments.

[0013] FIG. **5** is a timeline illustrating defined variables and intervals in circumstances where a most recent certificate was renewed before a last CRL update was received, and the certificate expired before the current time, according to some embodiments.

[0014] FIG. **6** is a timeline illustrating defined variables and intervals in circumstances where a most recent certificate was renewed after a last CRL update was received, and the certificate expiration date is beyond a permissible session end time, according to some embodiments.

[0015] FIG. **7** is a timeline illustrating defined variables and intervals in circumstances where a most recent certificate was renewed before a last CRL update was received, and the certificate has not yet expired, according to some embodiments.

[0016] FIG. **8** is a block diagram illustrating components of a device that functions as a relying party in a PKI communication network, according to some embodiments.

[0017] FIG. **9** is a general flow diagram illustrating a method that enables a trust relationship using an unexpired PKI certificate where a current status of the PKI certificate is unavailable, according to some embodiments.

[0018] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention.

[0019] The apparatus and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

DETAILED DESCRIPTION

[0020] According to some embodiments of the present invention, a method enables a trust relationship using an unexpired public key infrastructure (PKI) certificate, where a current status of the PKI certificate is unavailable. The method includes determining at a relying party that a certificate status update for the PKI certificate is unavailable. Next, in response to the certificate status update being unavailable, a tolerable certificate status age (TCSA) for the PKI certificate is determined at the relying party based on one or more attributes associated with a certificate holder of the PKI certificate. Using the PKI certificate, a trust relationship is enabled between the relying party and the certificate holder after determining the TCSA and before an expiration of the TCSA.

[0021] Embodiments of the present invention thus enable a relying party to continue to use an unexpired PKI certificate when connectivity to a corresponding certificate authority (CA) is unavailable. The TCSA is a length of time an unexpired certificate can be conditionally trusted in spite of a lack of a timely certificate status update. As described in detail below, the TCSA can be determined intelligently based on various attributes associated with the certificate holder. Thus, rather than precluding all use of certificates when connectivity to a corresponding CA is lost, or simply establishing an arbitrary grace period during which non-updated or expired certificates can be used, embodiments of the present invention enable a compromise that can improve communication network effectiveness while reducing communication network security risks.

[0022] Referring to FIG. **1**, a diagram illustrates a communication network **100** that includes open communication channels between a relying party **105**, a certificate holder **110**, a validation authority (VA) **130**, and a certification authority (CA) **115**. The certificate holder **110** is responsible for maintaining validity of a certificate **120** through certificate renewal with the CA **115**, or update operations with the CA **115** or the VA **130**. The relying party **105** is assumed to possess a latest valid public key of the CA **115** obtained through a secure channel, and hence is able to validate any certificate issued by the CA **115** and signed using a corresponding private key of the CA **115**. Also, the relying party **105** periodically receives certificate status update information from the CA **115**. For example, such status update information may be received by the relying party **105** directly from the CA **115** in the form of a certificate revocation list (CRL) **125**. Alternatively, as shown by the dashed lines in FIG. **1**, the relying party **105** may obtain the status update information indirectly by sending an online certificate status protocol (OCSP) query to a validation authority (VA) **130**, where the VA **130** receives the CRL **125** directly from the CA **115**.

[0023] When the certificate holder **110** attempts to gain access to resources of the relying party **105**, the certificate holder **110** presents its most up-to-date certificate **120** signed by the CA **115**, which is trusted by both the certificate holder **110** and the relying party **105**. The relying party **105** then verifies the validity of a signature of the CA **115**, and checks if the certificate **120** is identified in the CRL **125** received most recently from the CA **115**. If the certificate **120** carries a valid signature and is not included in the CRL **125** (i.e., it has not been revoked), the relying party **105** may accept the certificate **120** and grant resource access to the certificate holder **110**. Otherwise, the request for access to resources of the relying party **105** is denied.

[0024] However, establishing trust according to the conventional PKI communications illustrated in FIG. **1** is not possible if communication links with the CA **115** are unavailable. For example, consider that the communication network **100** comprises an ad hoc wireless communication network operated by various emergency response units at an incident scene, such as at a site destroyed by a hurricane or a terrorist attack. In such an environment, local back-end communication infrastructure may have been destroyed or be otherwise inoperable. Thus the certificate holder **110** and/or the relying party **105**, who may be members of different response units that need to communicate with each other, may not have connectivity with the CA **115**.

[0025] According to embodiments of the present invention, a relying party can continue to use an unexpired PKI certificate even when connectivity to a corresponding certificate authority (CA) is unavailable. However, use of PKI certificates is not merely extended arbitrarily, which could lead to breaches in network security.

[0026] Communication networks that implement embodiments of the present invention can comprise various types of wired or wireless network architectures including a mesh enabled architecture (MEA) network, or an Institute of Electrical and Electronics Engineers (IEEE) 802.11 network (i.e. 802.11a, 802.11b, 802.11g, 802.11n). (Note: for any IEEE standards recited herein, see: http://standards.ieee.org/getieee802/index.html or contact the IEEE at IEEE, 445 Hoes Lane, PO Box 1331, Piscataway, N.J. 08855-1331, USA.) It will be appreciated by those of ordinary skill in the art that such wireless communication networks can alternatively comprise any packetized communication network where packets are forwarded across multiple wireless hops. For example, such a wireless communication network can be a network utilizing multiple access schemes such as OFDMA (orthogonal frequency division multiple access), TDMA (time division multiple access), FDMA (Frequency Division Multiple Access), or CSMA (Carrier Sense Multiple Access).

[0027] Embodiments of the present invention enable a holder of a certificate to negotiate with a relying party for extension of a temporarily unverifiable trust relationship subject, such as under predetermined conditions on access or task authorization. For example, consider that a trust relationship is temporarily unverifiable due to delay in a certificate status update by a certification authority (CA) or a validation authority (VA), and/or a delay in a certificate renewal by a CA. Such delay can be caused by loss of connectivity to the CA and/or VA, for example.

[0028] The collection of PKI entities that need to be contacted for timely trust management, such as a CA or a VA, are referred to herein as a PKI Authority (PA). Further, if an entity is able to communicate with a PA, then it is referred to herein as being in an "on-line" state; if not, it is referred to herein as being in an "off-line" state. If the certificate holder is off-line, it will not be able to renew or update its certificate timely to avoid validation failure. If the relying party is off-line, it may not have an up-to-date CRL to determine if the certificate shown by the certificate holder has been revoked or not. A certificate that fails validation is normally revoked, unless there is successful conditional validation as enabled by the present invention. A certificate is valid, and hence trustworthy, from the time it is issued to the time it expires or is revoked, at which time the certificate may be renewed (in the case of expiration) or updated (in the case of revocation).

[0029] Referring to FIG. **2**, a certificate timeline **200** illustrates a need for a tolerable certificate status age (TCSA) and a certificate grace period (CGP) of a PKI certificate, according to some embodiments of the present invention. A TCSA may be needed before a certificate expires, whereas a CGP may be needed after a certificate expires. Consider that time progresses in the timeline **200** from left to right, and at a time **205** a certificate status update (provided, for example, through a CRL publication or an on-demand request) is received by a relying party, then at a time **210** the relying party loses connectivity with a PA, and a time **215** represents a current time. The period between the time **205** and the time **215** is a period during which the relying party did not receive a report of a revocation of the certificate. Between the time **205** and the time **210**, the relying party may assume that the certificate remains valid since a report of a revocation of the certificate could have been received by the relying party. Between the time **210** and the time **215**, the relying party could not receive any report from the PA, and hence any certification revocation would have been undetected by the relying party. The time **210** may not be determinable by the relying party at the current time **215**. Thus, the time **205** defines the beginning of a TCSA according to some embodiments of the present invention. Further, consider that the certificate is set to expire at a time **220** and that the relying party requires use of the certificate during a desired session that expires at a time **225**. The time **220** therefore defines a latest ending time of the TCSA to allow conditional validation of the unverifiable certificate. Further, the ending time of the TCSA is bounded from below by the time **215**, which is the current time. Subject to the above conditions, the relying party determines an ending time of the TCSA based on local policy. Further, the period between the time **220** and the time **225** represents a grace period that is required to cover a "validity gap" between the expiration of the certificate and the end of the desired session, during which the relying party is willing to conditionally regard the certificate as valid (i.e., willing to accept the recently expired certificate for enabling a trust relationship).

[0030] Referring to FIG. **3**, a certificate state diagram illustrates five possible states of a certificate, according to some embodiments of the present invention. An unknown state **305** applies after a certificate is granted and before it is validated, renewed or revoked. A good state **310** applies after a certificate is validated and before it expires, fails to be validated as needed, or is revoked. A certificate in the good state **310** may remain in the good state **310** if it can be conditionally validated. An expired state **315** applies after expiration of a validity period if a grace period has not been granted. An extended state **320** applies if a validity period has expired but a grace period has been granted and has not expired, and the certificate has not been renewed. Finally, a revoked status **325** applies if a certificate has expired or been revoked, or an applicable grace period has expired or been denied, and the certificate has not been renewed. The expired state **315** and the extended state **320** add to three certificate states of good, revoked and unknown that are defined according to the prior art in the online certificate status protocol (OCSP), as described in M. Myers et al., "X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol—OCSP", Internet RFC 2560, June 1999.

[0031] According to some embodiments of the present invention, a certificate status history associated with a certificate can be used to define a TCSA and a grace period. For example, each certificate issued by a CA to a certificate holder may include, in addition to the identity and public key of the certificate holder, the information included in Table 1 below:

TABLE 1

Variable	Definition
T_BeginSeniority	Earliest time from which the certificate holder's certificate (or authorization status) has not been involuntarily revoked.
T_BeginValid	Time when the certificate holder's oldest certificate was renewed after the most recent validity gap.
T_LastRenew	Time when the certificate holder's most recent certificate was renewed.
T_LastExpire	Expiration time of the certificate holder's most recently renewed certificate.
MaxOutdate	Maximum permissible length of time an unexpired certificate can be conditionally trusted in spite of a lack of timely certificate status update. This variable is set by policy and bounds the calculated tolerable certificate status age. This parameter can be used for any certificate holder.
MaxGracePeriod	Maximum permissible length of time that a certificate may be conditionally granted valid status even though it has expired. This variable is set by policy and bounds the calculated certificate grace period that can be extended to any certificate holder.
MaxSessionLength	Maximum permissible length of a session starting from the current time.

[0032] Some organizations or network management systems may want to impose an upper-bound on the time elapsed since a relying party most recently obtained a certificate status update and during which the relying party can authenticate a certificate holder. This upper-bound ensures that a certificate status update is acceptably fresh to be considered reliable. MaxOutdate is a variable determined by local policy to achieve this.

[0033] In normal circumstances, a CA may stop monitoring a certificate after the certificate has expired. However, because a relying party may be able to grant a certificate grace period to a certificate holder, there may be a need to continue monitoring the certificate beyond its expiration time for possible revocation. In accordance with some embodiments of the present invention, the CA determines a maximum certificate grace period for each certificate the CA issues. When a certificate expires, the CA will continue to monitor the certificate over this length of time for possible revocation. Also, a certificate grace period granted by a relying party generally will not exceed the maximum certificate grace period. This maximum certificate grace period is included in the certificate for synchronization with the relying party.

[0034] When a holder of an expired certificate presents the certificate to a relying party for authentication service, with an implicit request for a certificate grace period, the certificate holder may additionally indicate a session length over which the certificate grace period would desirably cover. Some organizations may want to impose an upper-bound on session length that may be accommodated by a relying party for a certificate holder with an expired certificate. This upper-bound essentially limits an extent of security compromise due to potential mistakes in granting a certificate grace period to an undeserving certificate holder. MaxSessionLength is a variable determined by local policy to achieve this.

[0035] By time-stamping each certificate revocation list (CRL) update received from a CA, a relying party knows or can derive at least the following variables included in Table 2.

TABLE 2

Variable	Definition
T__LastCRL	Time the last CRL update was received.
T__BeginUncertainty	max(T__LastRenew, T__LastCRL).
T__EndUncertainty	min(T__Current + MaxSessionLength, T__LastExpire + MaxGracePeriod).

[0036] T_Current denotes the current time at the moment when a certificate holder is attempting to authenticate with a relying party. The interval from T_BeginUncertainty to T_EndUncertainty represents an interval in which the relying party is unable to detect a revocation of the certificate, if any. It is assumed that the relying party has a valid public key of the CA and any necessary certificate chains, and hence is able to validate all the information contained in any certificate signed with a corresponding private key of the CA. When a relying party is presented with an unexpired certificate that the relying party cannot verify timely, the relying party will first determine an appropriate value for a tolerable certificate status age (TCSA) based on predetermined policy.

[0037] According to some embodiments of the present invention, intervals are defined as provided in Table 3 below.

TABLE 3

Interval	Notation	Definition
Uncertainty Interval	U	T__EndUncertainty − T__BeginUncertainty
Verifiable Recent Validity Interval	V	T__BeginUncertainty − T__BeginValid
Verifiable Seniority Interval	S	T__BeginUncertainty − T__BeginSeniority
Validity Evaluation Interval	E_V	T__EndUncertainty − T__BeginValid
Seniority Evaluation Interval	E_S	T__EndUncertainty − T__BeginSeniority

[0038] Referring to FIG. **4**, a timeline **400** illustrates the above defined variables and intervals in circumstances where a most recent certificate was renewed after a last CRL update was received, and the certificate expired before the current time. The rectangles C_1 to C_4 each indicate the valid lifetime of a certificate.

[0039] Referring to FIG. **5**, a timeline **500** illustrates the above defined variables and intervals in circumstances where a most recent certificate was renewed before a last CRL update was received, and the certificate expired before the current time.

[0040] Referring to FIG. **6**, a timeline **600** illustrates the above defined variables and intervals in circumstances where a most recent certificate was renewed after a last CRL update was received, and the certificate expiration date is beyond a permissible session end time.

[0041] Referring to FIG. **7**, a timeline **700** illustrates the above defined variables and intervals in circumstances where a most recent certificate was renewed before a last CRL update was received, and the certificate has not yet expired.

[0042] Predetermined personnel attributes associated with a certificate holder can be included in the certificate holder's certificate, such that the attributes can be used by a relying party to further determine the trustworthiness of the certificate holder. For example, such personnel attributes can include the following:

- **[0043]** Security Level: A security level of the certificate holder, which may indicate that a predetermined level of background investigation has taken place, and that actual vetting of the certificate holder's trustworthiness has been accomplished. A security level may provide a reliable measure of trustworthiness.
- **[0044]** Security Tenure: A length of time a certificate holder is authorized to operate at a given security level, which may be based on a reasonable assumption that the longer the certificate holder has been at a given security level the more trustworthy the certificate holder may be for the authentication required to operate at the given security level.
- **[0045]** Total Employment Seniority: This attribute may be based on a reasonable assumption that the longer a certificate holder has worked for an employer the more trustworthy the certificate holder may be.
- **[0046]** Rank: This attribute may be based on a reasonable assumption that certificate holders of higher ranks are often more trustworthy and hence given more responsibility.

[0047] Trustworthiness Metric: Rather than having to infer a level of trustworthiness from selected attributes, it is also possible for an organization to assign a certificate holder a specific trustworthiness metric, which represents an explicit level of trustworthiness that is preapproved by the organization.

[0048] The above are examples only of the type of attributes that can be used to help a relying party determine the trustworthiness of a certificate holder and hence a TCSA or a grace period that should be allocated to the certificate holder depending on whether the certificate is unexpired or expired. Other attributes, or combinations or subsets of the attributes also can be used within the scope of the present invention. For example, an organization may value Total Employment Seniority more than Rank, and therefore would include Total Employment Seniority in a certificate but leave Rank out. Of course, it would also be possible to create a function of one or more such attributes. The specific attributes used and any functions thereof can be a matter of local policy.

[0049] According to some embodiments of the present invention, system attributes associated with a device utilized by a certificate holder are used to implement algorithms of the present invention. For example, a relying party may derive a trustworthiness metric value based on predetermined system attributes of the device used by a certificate holder, wherein said system attributes are verifiable by the relying party through physical contact with the certificate holder.

[0050] One example of an implementation of such a trustworthy metric is based on whether the device is equipped with licensed hardware (e.g., a secure storage device for the private key, or a secure device that executes all public key cryptography operations) or licensed software (e.g., special encryption software) that can be verified through physical contact.

[0051] Given that a certificate holder is able to demonstrate evidence that its device possesses the needed attributes, the relying party then reserves a right to grant the certificate holder a TCSA or a grace period (depending, respectively, on whether the certificate is unexpired or expired), which are subject to specific conditions on access or task authorization according to a predetermined policy, as well as the maximum TCSA or maximum grace period defined in the certificate.

[0052] Further, environmental attributes can be used to implement algorithms of the present invention. In some embodiments, it may be appropriate to consider environmental attributes when deciding whether or not to grant a TCSA or a grace period (depending on whether the certificate is unexpired or expired), and when determining how long such a TCSA or grace period should be. For example, such environmental attributes can include:

[0053] Network Status: This may include the accessibility of a certificate status repository.

[0054] Detected Alarms: This may include a flag in a wireless local area network (WLAN) or worldwide interoperability for microwave access (WiMax) beacon that indicates an elevated state of alert.

[0055] Local Policy Variables: This may include a locally configurable flag that states, for example, that the certificate holder is at an incident scene of unusual proportions or duration.

[0056] Using the above environmental attributes, an organization may institute a policy that states, for example, that no grace period will be granted unless both of the following conditions are met: 1) local policy variables at the relying party indicate that the certificate holder is present at an incident, and 2) an authoritative CRL for a responsible agency is not reachable via the network.

[0057] As a certificate could have been renewed since T_LastCRL, the starting time for a TCSA is T_BeginUncertainty, which is max(T_LastRenew, T_LastCRL). For a TCSA to be considered valid by a relying party, the ending time for the TCSA is after T_Current but before T_LastExpire. If T_LastExpire is before T_Current, TCSA is not applicable since the certificate has already expired. Further, the ending time for the TCSA must be before (T_BeginUncertainty+MaxOutdate). Thus, provided that the certificate is unexpired (i.e., T_Current<T_LastExpire), a valid TCSA satisfies the following bounds:

$$TCSA \geqq T\_\mathrm{Current} - T\_\mathrm{BeginUncertainty}; \qquad \text{Eq. 1}$$

$$TCSA \leqq \mathrm{Max}TCSA, \qquad \text{Eq. 2}$$

where

$$\mathrm{Max}TCSA = \min(\mathrm{MaxOutdate}, (T\_\mathrm{LastExpire} - T\_\mathrm{BeginUncertainty})). \qquad \text{Eq. 3}$$

Otherwise, if the certificate has expired (i.e., T_Current≧T_LastExpire), TCSA is set to 0.

[0058] According to some embodiments of the present invention, a TCSA can be determined by a mathematical function of metrics assigned to each of the applicable attributes. For example, a mathematical function for TCSA can be defined as follows:

If T_Current<T_LastExpire, then

$$TCSA = (T\_\mathrm{Current} - T\_\mathrm{BeginUncertainty}) + T(\mathrm{attributes}), \qquad \text{Eq. 4}$$

else TCSA=0.

T(attributes) conforms to the following bounds:

$$0 \leqq T(\mathrm{attributes}) \leqq \mathrm{Max}TCSA - (T\_\mathrm{Current} - T\_\mathrm{BeginUncertainty}). \qquad \text{Eq. 5}$$

[0059] Also, a variable (x(attributes) can be defined to be T(attributes) normalized by the upper-bound above, so that 0≦α(attributes)<1. Specifically,

$$\alpha(\mathrm{attributes}) = T(\mathrm{attributes}) / \Delta TCSA, \qquad \text{Eq. 6}$$

where

$$\Delta TCSA = (\mathrm{Max}TCSA - (T\_\mathrm{Current} - T\_\mathrm{BeginUncertainty})) \qquad \text{Eq. 7}$$

Then, provided the certificate is unexpired,

$$TCSA = (T\_\mathrm{Current} - T\_\mathrm{BeginUncertainty}) + \alpha(\mathrm{attributes}) \times \Delta TCSA. \qquad \text{Eq. 8}$$

[0060] In one embodiment, (x(attributes) can be a minimum of metrics assigned to individual applicable attributes, wherein each metric is a variable bounded between 0 and 1. In another embodiment, (x(attributes) can be a product of the metrics.

[0061] According to some other embodiments of the present invention, a TCSA can be determined by referring to a table, such as Table 4 below.

TABLE 4

Personnel Attributes		System Attributes	Environmental Attributes	Result
Tenure	Rank	Secure Hardware?	Network Status	TCSA
*	*	*	PA Reachable	min(MaxTCSA, 20 Minutes)
≦1 Year	Lower than or equal to rank of Captain	No	PA Unreachable	min(MaxTCSA, 1 Hour)
≦1 Year	Higher than rank of Captain	No	PA Unreachable	min(MaxTCSA, 1 Day)
>1 Year	Lower than or equal to rank of Captain	No	PA Unreachable	min(MaxTCSA, 1 Day)
>1 Year	Higher than rank of Captain	No	PA Unreachable	min(MaxTCSA, 5 Days)
≦1 Year	Lower than or equal to rank of Captain	Yes	PA Unreachable	min(MaxTCSA, 2 Hours)
≦1 Year	Higher than rank of Captain	Yes	PA Unreachable	min(MaxTCSA, 2 Days)
>1 Year	Lower than or equal to rank of Captain	Yes	PA Unreachable	min(MaxTCSA, 2 Days)
>1 Year	Higher than rank of Captain	Yes	PA Unreachable	min(MaxTCSA, 10 Days

[0062] In general, a TCSA can be a function of personnel attributes, system attributes, environmental attributes, MaxOutdate, as well as any other aforementioned variables or an equivalent.

[0063] Also, according to some embodiments of the present invention, a certificate grace period (CGP) begins at T_LastExpire, and ends no later than (T_LastExpire+MaxGracePeriod). Further, it is desirable that the CGP ends no later than (T_Current+MaxSessionLength). Hence, the CGP will end no later than T_EndUncertainty, which is a minimum of (T_LastExpire+MaxGracePeriod) and (T_Current+MaxSessionLength). If (T_EndUncertainty −T_LastExpire)≧0, then the CGP is bounded by (T_EndUncertainty−T_LastExpire). However, if (T_EndUncertainty−T_LastExpire)<0 (e.g., as shown in FIG. **3**), then the CGP is set to 0 since the certificate will remain unexpired throughout the period of MaxSesionLength. Hence, the CGP satisfies the following bounds:

$$0 \leqq CGP \leqq \max(T\_\mathrm{EndUncertainty} - T\_\mathrm{LastExpire}, 0) \qquad \text{Eq. 9}$$

[0064] According to some embodiments of the present invention, a CGP is determined based on a trustworthiness metric, β(*), whose value is bounded between 0 and 1. Specifically, the CGP conforms to the following equations.

$$X = \beta(*) \times \mathrm{MaxGracePeriod}; \qquad \text{Eq. 10}$$

$$Y = \max(T\_\mathrm{EndUncertainty} - T\_\mathrm{LastExpire}, 0); \qquad \text{Eq. 11}$$

$$CGP = \min(X, Y). \qquad \text{Eq. 12}$$

[0065] One example of an implementation of a trustworthiness metric is based on the Verifiable Recent Validity Interval. Given that a certificate holder is able to demonstrate evidence that it has been trustworthy over a continuous interval, the relying party reserves a right to grant the certificate holder a grace period, which is subject to specific conditions on access or task authorization according to a predetermined policy. Specifically, a trustworthiness metric called a Normalized Verifiable Recent Validity Interval (V*) is defined as the Verifiable Recent Validity Interval, normalized by a Validity Evaluation Interval, as defined in the following equation:

$$V^* = \frac{V}{E_V} = \frac{V}{V + U} \qquad \text{Eq. 13}$$

[0066] Therefore, V* takes a value between 0 and 1. The certificate grace period granted by the relying party is a non-decreasing function of V*, upper-bounded by the maximum grace period as defined in the certificate. In particular, the trustworthiness metric is a function of V and U, and a certificate grace period can be derived from Eq. 10, Eq. 11, and Eq. 12, by setting the trustworthiness metric β(*) to V*.

[0067] Another example of an implementation of a trustworthiness metric is based on the Verifiable Seniority Interval. Given that a certificate holder is able to demonstrate evidence that it has a verifiable history of receiving certificates from the same CA without having been involuntarily revoked, the relying party reserves a right to grant the certificate holder a grace period, which is subject to specific conditions on access or task authorization according to a predetermined policy. Specifically, a trustworthy metric called a Normalized Verifiable Seniority Interval (S*) is defined as the Verifiable Seniority Interval, normalized by a Seniority Evaluation Interval, as defined in the following equation:

$$S^* = \frac{S}{E_S} = \frac{S}{S + U} \qquad \text{Eq. 14}$$

[0068] Therefore, S* takes a value between 0 and 1. The certificate grace period granted by the relying party is a non-decreasing function of S*, upper-bounded by the maximum grace period as defined in the certificate. In particular, the trustworthiness metric is a function of S and U, and a certificate grace period can be derived from Eq. 10, Eq. 11, and Eq. 12, by setting the trustworthiness metric β(*) to S*.

[0069] According to some other embodiments of the present invention, a trustworthiness metric, and hence a CGP, can be determined as a function of personnel attributes, system attributes, and environmental attributes. For example a trustworthiness metric can be determined by referring to a table, such as Table 5 below.

TABLE 5

Personnel Attributes		System Attributes Secure	Environmental Attributes	Result Trust-worthiness
Tenure	Rank	Hardware?	Network Status	Metric
*	*	*	PA Reachable	0.05
≦1 Year	Lower than or equal to rank of Captain	No	PA Unreachable	0.10
≦1 Year	Higher than rank of Captain	No	PA Unreachable	0.25
>1 Year	Lower than or equal to rank of Captain	No	PA Unreachable	0.25
>1 Year	Higher than rank of Captain	No	PA Unreachable	0.75
≦1 Year	Lower than or equal to rank of Captain	Yes	PA Unreachable	0.20
≦1 Year	Higher than rank of Captain	Yes	PA Unreachable	0.50
>1 Year	Lower than or equal to rank of Captain	Yes	PA Unreachable	0.50
>1 Year	Higher than rank of Captain	Yes	PA Unreachable	1.00

[0070] In general, the certificate grace period is a function of V, S, U, and MaxGracePeriod, as well as any other aforementioned variables and attributes, or an equivalent.

[0071] According to some embodiments of the present invention, implicit negotiation is used, wherein negotiation between a certificate holder and a relying party is implied when the certificate holder presents to the relying party an unverifiable certificate. In this respect, the relying party will assume that negotiation is in order by default. For example, further to a need for requesting access to a relying party's resources while a service of a CA is unavailable, a certificate holder may present its PKI certificate, which includes predetermined certificate attributes, to the relying party. After receiving the PKI certificate, knowing that the CA service is unavailable, the relying party determines an appropriate TCSA or grace period for the certificate holder based on the predetermined certificate attributes and whether the certificate has expired.

[0072] For determination of a certificate grace period, explicit negotiation can alternatively be used, wherein a negotiation handshake between a certificate holder and a relying party is required prior to an authentication request from the certificate holder to the relying party. In this respect, the relying party will assume that negotiation is only executed on demand. For example, further to a need for requesting access to a relying party's resources while a service of a CA is unavailable, a certificate holder may initiate a trust negotiation handshake with the relying party. The handshake contains steps for the certificate holder to provide to the relying party evidence or attributes required to negotiate an extension of the certificate holder's grace period, depending on whether the certificate has expired. After a grace period is determined (depending on whether the certificate is unexpired or expired), a normal certificate based authentication process is started between the certificate holder and the relying party, without the need of a CA service in certificate verification.

[0073] Referring to FIG. **8**, a block diagram illustrates components of a device **800** that functions as a relying party in a PKI communication network, according to some embodiments of the present invention. The device **800**, for example, can be an integrated unit such as a computer, mobile telephone, or personal digital assistant (PDA) containing at least all the elements depicted in FIG. **8**, as well as any other elements necessary for the device **800** to perform its particular functions. Alternatively, the device **800** can comprise a collection of appropriately interconnected units or devices, wherein such units or devices perform functions that are equivalent to the functions performed by the elements depicted in FIG. **8**.

[0074] The device **800** comprises a random access memory (RAM) **805** and a programmable memory **810** that are coupled to a processor **815**. The processor **815** also has ports for coupling to network interfaces **820**, **825**. The network interfaces **820**, **825**, which for example may be wireless network interfaces, can be used to enable the device **800** to communicate with other node devices in a communication network.

[0075] The programmable memory **810** can store operating code (OC) for the processor **815** and code for performing functions associated with a network device. For example, the programmable memory **810** can store computer readable program code components **830** configured to cause execution of a method for enabling a trust relationship using an unexpired PKI certificate, where a current status of the PKI certificate is unavailable, as described herein.

[0076] Referring to FIG. **9**, a general flow diagram illustrates a method **900** for enabling a trust relationship using an unexpired PKI certificate where a current status of the PKI certificate is unavailable, according to some embodiments of the present invention. First, at step **905**, a relying party determines that a certificate status update for the PKI certificate is unavailable. For example, the device **800** functioning as a relying party in a PKI communication network determines that connectivity with a PA concerning the certificate is not available.

[0077] Next, at step **910**, the relying party determines, in response to the certificate status update being unavailable, a tolerable certificate status age (TCSA) for the PKI certificate based on one or more attributes associated with a certificate holder of the PKI certificate. For example the device **800** determines a TCSA based on the attributes defined in Table 4.

[0078] At step **915**, using the PKI certificate, a trust relationship is enabled between the relying party and the certificate holder after determining the TCSA and before an expiration of the TCSA. For example, the device **800** enables a trust relationship with a wireless node operating in the PKI communication network as a certificate holder.

[0079] Advantages of some embodiments of the present invention therefore include enabling a relying party to continue to use an unexpired PKI certificate when connectivity to a corresponding certificate authority (CA) is unavailable. A balance thus can be made between strict enforcement of a certificate validation, which could have a negative impact on the availability of a PKI, and arbitrary allowance of a TCSA, which could compromise network security.

[0080] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of the present teachings. The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0081] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," "has", "having," "includes", "including," "contains", "containing" or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, or contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element preceded by "comprises a . . . ", "has a . . . ", "includes a . . .", or "contains a . . ." does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, or contains the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially", "essentially", "approximately", "about" or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0082] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and system described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used.

[0083] Moreover, an embodiment can be implemented as a computer-readable storage medium having computer readable code stored thereon for programming a computer (e.g., comprising a processor) to perform a method as described and claimed herein. Examples of such computer-readable storage mediums include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0084] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

We claim:

1. A method for enabling a trust relationship using an unexpired public key infrastructure (PKI) certificate where a current status of the PKI certificate is unavailable, the method comprising:

determining at a relying party that a certificate status update for the PKI certificate is unavailable;

determining at the relying party, in response to the certificate status update being unavailable, a tolerable certificate status age (TCSA) for the PKI certificate based on one or more attributes associated with a certificate holder of the PKI certificate; and

enabling, using the PKI certificate, a trust relationship between the relying party and the certificate holder after determining the TCSA and before an expiration of the TCSA.

2. The method of claim **1**, wherein the TCSA conforms to the following equation: TCSA=(T_Current−T_BeginUncertainty)+α(attributes)×ΔTCSA.

3. The method of claim **1**, wherein the one or more attributes associated with the certificate holder are selected from the following: one or more personnel attributes, one or more system attributes, and one or more environmental attributes.

4. The method of claim **3**, wherein the personnel attributes are identified in the PKI certificate and are selected from the following: a security level, a security tenure, a total employment seniority, a rank, and a trustworthiness metric.

5. The method of claim **3**, wherein the system attributes include whether a device associated with the PKI certificate includes licensed hardware or software.

6. The method of claim **5**, wherein the licensed hardware comprises a secure storage facility for a private key associated with the PKI certificate.

7. The method of claim **5**, wherein the licensed software comprises encryption software.

8. The method of claim **3**, wherein the environmental attributes are selected from the following: a network status, one or more detected alarms, and one or more local policy variables.

9. The method of claim **1**, wherein the attributes associated with the certificate holder are defined in the PKI certificate.

10. The method of claim **1**, wherein the relying party determines that a certificate status update for the PKI certificate is unavailable based on a failure to receive a response to a status request.

11. The method of claim **1**, wherein a maximum age of the TCSA is determined by a MaxOutdate variable.

12. A device for enabling a trust relationship using an unexpired public key infrastructure (PKI) certificate where a current status of the PKI certificate is unavailable, comprising:

a processor; and

a programmable memory coupled to the processor for storing:

computer readable program code components for determining at a relying party that a certificate status update for the PKI certificate is unavailable;

computer readable program code components for determining at the relying party, in response to the certificate status update being unavailable, a tolerable certificate status age (TCSA) for the PKI certificate based on one or more attributes associated with a certificate holder of the PKI certificate; and

computer readable program code components for enabling, using the PKI certificate, a trust relationship between the relying party and the certificate holder after determining the TCSA and before an expiration of the TCSA.

13. The device of claim **12**, wherein the TCSA conforms to the following equation: $TCSA=(T\_Current-T\_BeginUncertainty)+\alpha(attributes)\times\Delta TCSA$.

14. The device of claim **12**, wherein the one or more attributes associated with the certificate holder are selected from the following: one or more personnel attributes, one or more system attributes, and one or more environmental attributes.

15. The device of claim **14**, wherein the personnel attributes are identified in the PKI certificate and are selected from the following: a security level, a security tenure, a total employment seniority, a rank, and a trustworthiness metric.

16. The device of claim **14**, wherein the system attributes include whether a device associated with the PKI certificate includes licensed hardware or software.

17. The device of claim **16**, wherein the licensed hardware comprises a secure storage facility for a private key associated with the PKI certificate.

18. The device of claim **16**, wherein the licensed software comprises encryption software.

19. The device of claim **14**, wherein the environmental attributes are selected from the following: a network status, one or more detected alarms, and one or more local policy variables.

20. The device of claim **12**, wherein the attributes associated with the certificate holder are defined in the PKI certificate.

* * * * *