



- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
- (21) **International Application Number:**
PCT/MY2015/000053
- (22) **International Filing Date:**
21 July 2015 (21.07.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI2014702046 24 July 2014 (24.07.2014) MY
- (71) **Applicant:** MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventors:** ALWYN Goh; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). NG Kang Siong; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). SEA, Chong Seak; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). THILLAI, Raj T. Ramanathan; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** MOHAN K; Adastra Intellectual Property Sdn Bhd, A-28-10, Menara UOA Bangsar, No. 5, Jalan Bangsar Utama 1, 59000 Kuala Lumpur (MY).

- (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) **Title:** METHOD AND SYSTEM FOR COMPUTATION AND VERIFICATION OF AUTHENTICATION PARAMETERS FROM INDEPENDANT MEASUREMENTS OF TIME OR LOCATION

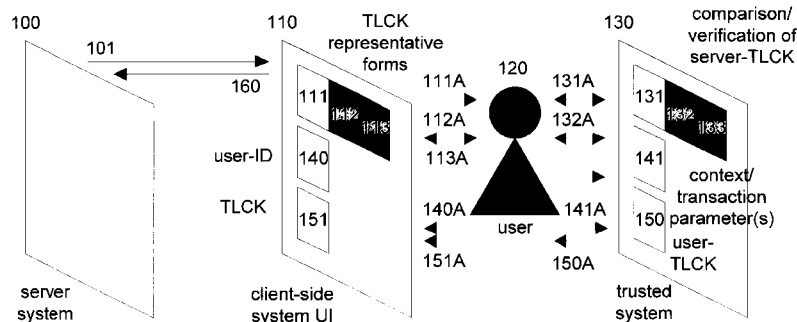


FIGURE 1

(57) **Abstract:** The present invention discloses a method and system for computation and verification of authentication parameters between two entities, an originating entity and a receiving entity, which in the embodiment of interest comprises a server (100), a client interface thereof (110), a human user (120) and a trusted system (130) deemed as such by the human user. The method comprises the user (120) authenticating the server (100) by visual comparison of an authentication code in numeric, symbolic, graphical or visual-interactive form computed by the server (100) in comparison to a plurality of reference codes computed on the trusted system (130); and reciprocally the server (100) authenticating the user (120) subsequent to transcription or transfer of an authentication code, as computed and displayed on the trusted system (130), to the client interface (110) and thenceforth to the server (100), by means of comparison of the test code to a plurality of reference codes computed on the server (100). The method of computation and verification of the authentication codes as aforesaid are by means of zero knowledge (ZK) transformation of time, location or service-specific information; with measurement or determination of time or location information as independently undertaken on server (100) and trusted system (130).

**METHOD AND SYSTEM FOR COMPUTATION AND VERIFICATION OF
AUTHENTICATION PARAMETERS FROM INDEPENDANT
MEASUREMENTS OF TIME OR LOCATION**

5 FIELD OF INVENTION

The present invention relates generally to a method and system for computation and verification of authentication parameters between two entities, an originating entity and a receiving entity, more particularly a
10 method and system for computation and verification of authentication parameters from independent measurements of time or location, and specification thereof based on configurable constraints on such measurement differences.

15 BACKGROUND ART

At present existing one-time key (OTK) or password (OTP) solutions require a client-side generation on specialised devices or alternatively a server-side generation and subsequent transmission via Short Messaging
20 System (SMS) to previously specified cellular phones.

These provide sole use for client-to-server authentication, without addressing the reciprocal process of server-to-client authentication, and are susceptible to man-in-the-middle (MITM) attacks, and consequent
25 transaction fraud. These are also highly dependent on tight synchronisation between time measurements as executed on different systems and devices. Present methods utilize repeated, and possibly unauthorised, use of generated OTK within specified time-frame. In addition to this, present methods are vulnerable, in that the pair-wise
30 secret-keys used for OTK generation are vulnerable, which results in

single-points of weakness in operational systems. This leads to inflexibility with respect to management of keys for OTK generation, resulting in high costs required to undertake initial deployments and subsequent operations.

SUMMARY OF INVENTION

The present invention provides a method and system for mutual authentication between two entities. The present invention proposes a method and system for computation and verification of authentication parameters from independent measurements of time or location, and specification thereof based on configurable constraints on such measurement differences.

10 In one aspect of the present invention is a method and system for computation and verification of authentication parameters between two entities, an originating entity and a receiving entity, upon initiating an interaction by the originating entity, a server or a client initiating a service request over a communications network which will be received by the receiving entity, the client or the server. The method comprises the client authenticating the server by visual comparison of an authentication code in numeric, symbolic or graphical form computed by the server to a plurality of the corresponding reference codes computed on a trusted application; and the server authenticating the client by manual transcription of an authentication code computed and displayed on the trusted application and comparison of the test code to a plurality of reference codes computed on the server.

25 According to the embodiments of the present invention, computation of the authentication code by the server and the trusted application is based on a Zero-Knowledge (ZK) transformation which further comprises the transformation of key information which is securely managed and rigorously associated to either the server or the client; service information derived from the service request or a subsequent grant; time or location information measured or inferentially computed independently by either

the server or the client; and an evaluation of the authentication code received from either the server or the client based on computation of the plurality of reference codes based on predetermined approximation of time and location such that the authentication code is equal to one of the
5 plurality of reference codes.

The trusted application comprises an application operating on a mobile device or computer workstation that does not have connectivity to the communications network or a direct connectivity the server. The time
10 information measured or inferentially computed independently further comprises measuring of a plurality of measurement values by independently operated and calibrated system clocks capable of producing measurement values that differ and if the difference exceeds a predetermined maximum degree, authentication fails. The location
15 information measured or inferentially computed independently further comprises computations of Global Positioning System (GPS) signals as received by the trusted application or communications parameters which comprises protocol identifiers associated with Internet access, including addresses associated with the service request initiated the client and
20 network connectivity, including addresses associated with access points for wireless access points and cellular base stations.

Computation of the authentication code by the server and the trusted application is based on Zero-Knowledge (ZK) integration which further
25 comprises the input of key information associated to the originating entity; and predetermined approximation of time or location measured independently on the originating entity.

Verification of the authentication code by the server and the trusted
30 application is computed as a Zero-Knowledge (ZK) query which further

comprises the input of key information associated to the receiving entity;
predetermined approximation of time or location measured independently
on the receiving entity; and predetermined plurality of extrapolations of
time or location based on the independent measurement on the originating
5 entity.

In a further embodiment of the present invention, the method further
comprises computation of a reciprocal authentication code that integrates
additional inputs associated with service information including a received
10 authentication code. The method further comprises verification of a
reciprocal authentication code that integrates additional inputs associated
with service information including a transmitted authentication code.

The authentication code is computed on the server and received by the
15 client in numeric, symbolic or graphical form suitable for use by the client,
comprises visual comprehension of the authentication code; manual
transcription of the authentication code into the trusted application by
means of numeric, symbolic or graphical data entry; visual or computer
assisted comparison of the authentication code against the plurality of
20 reference codes computed on the trusted application; and manual or
computer assisted determination as to whether the authentication code is
authentic proof of the server identity.

The authentication code is computed on the server and received by the
25 client in numeric, symbolic or graphical form suitable for sequential
application by the client, comprises requesting for generation of a
corresponding verification code on the trusted application; visual
comparison of the authentication code and the plurality of reference codes
as computed on the trusted application system; and manual or computer-

assisted determination as to whether the authentication code is authentic proof of the server identity.

The authentication code associated with the server in visual or graphical
5 form and the corresponding verification code as computed on the trusted application depend on progressive and interactive computation, wherein visual comparison of the authentication and the plurality of reference codes are executed as an iterative and interactive sequence.

10 The authentication code is computed on the server and received by the client in an image or graphical form suitable for use by the client, comprises transferring onto the trusted application by means of a camera or an equivalent imaging device attached to a hardware platform on which the trusted application is operating or equivalent transfer of designated
15 image or graphical data directly to the trusted application; and verification within the trusted application of the received authentication code against the plurality of reference codes as computed; and indicating to the client as to whether the authentication code is authentic proof of the server identity.

20

The reciprocal authentication code is computed and transmitted, upon acceptable determination of the server authenticity in numeric or symbolic form suitable for use by the client, comprises manual or automatic transcription into the trusted application by means of numeric or symbolic
25 data entry of additional inputs associated with service information; visual comprehension of the reciprocal authentication code as computed on the trusted application; visual or computerised transcription of the reciprocal authentication code into the server interface component by means of numeric or symbolic data entry; transmission of transcribed reciprocal
30 authentication code to the server by means of the communications

network; automatic comparison of the received authentication code against the plurality of reference codes computed on the server; and automatic determination as to whether the authentication code is authentic proof of the client commitment to the service.

5

The computation and verification of the authentication code requires the originating entity and the receiving entity to be able to access a secret-key as used in symmetric-key cryptographic protocols, and the secret-key is exclusively and irrefutably associated to the originating entity.

10

The secret-key used for computation of the authentication code is associated to a key-pair as used in asymmetric-key cryptographic protocols, whereby a private-key of the key-pair is exclusively and irrefutably associated to the originating entity and the corresponding
15 public-key of the key-pair is accessible to the receiving entity prior to initiating interactions.

The use of the secret-key or the private-key by the originating entity or the receiving entity is subject to rigorous control necessitating Zero-
20 Knowledge (ZK) demonstration of at least one constituent key-factors associated to the originating entity, comprising a secret password that is in the exclusive knowledge of the user; or numeric or symbolic parameters uniquely associated to the server or the client.

25 The use of the secret-key or the private-key depends on Zero-Knowledge (ZK) demonstration of a plurality of constituent key-factors, as subject to configuration prior to initiating interactions.

The client is associated with a plurality of trusted applications being
30 utilised for computation and verification of the authentication code,

comprising the client being able to rigorously and irrefutably demonstrate access to one or more of the plurality of constituent key-factors.

The public-key associated with the server is accessible to the client prior
5 to initiating interactions between the server and the client.

The originating entity or the receiving entity computes a cryptographic signature as a Zero-Knowledge (ZK) integration of inputs which comprise the secret-key to be further utilized for a subsequent computation of
10 authentication codes by the originating entity or the receiving entity; or the private-key previously associated with the originating entity or the receiving entity; allowing the outcome of the computation to be unambiguously and irrefutably verified by a plurality of other entities in prior possession of the corresponding public-key to the effect that the
15 originating entity or the receiving entity is deemed to have undertaken associative commitment with respect to being associated to the secret-key.

The computation of a cryptographic secure-message as a Zero-
20 Knowledge (ZK) integration of inputs which further comprises the public-key associated with the receiving entity as expressly specified by the originating entity; such that verification of the outcome of the computation equivalently comprises the private-key corresponding to the public-key previously utilised by the originating entity to effect that recovery of the
25 secret-key from the outcome parameter and consequent verification thereof can only be undertaken by the receiving entity.

The computation of the cryptographic signature or secure-message is by the server, and transmitted to the trusted application to enable consequent
30 computation of the secret-key specific to the interaction to enable correct

demonstration on the trusted application of the private-key, with equivalent computation independently undertaken on the server in relation to the interaction.

- 5 The reciprocal authentication code is computed using the session-key specific to the interaction as independently computed on the server and the trusted application engaged in the interaction.

The secret or the public-key associated with the originating entity or the
10 receiving entity depends on computation of the cryptographic signature or secure-message by a trusted third-party (TTP) system, wherein the trusted third-party (TTP) is deemed to be trustworthy; and further that the trusted third-party (TTP) public-key is accessible to the originating entity and the receiving entity prior to the interaction.

15

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it is being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the
20 advantages of the present invention.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by
5 references to specific embodiments thereof, which are illustrated, in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying
10 drawings in which:

FIGURE 1 illustrates a preferred embodiment of a method and system for computation and verification of authentication parameters between two entities.

15

FIGURE 2 illustrates an embodiment of the present invention with visual interactive verification.

FIGURE 3 illustrates an embodiment of the present invention with
20 computer-assisted verification, with consequent interaction-specific key.

FIGURE 4 illustrates computation Z , and recovery Z' , of cryptographic signature or secure-messages.

25 FIGURE 5 illustrates independent establishment Z'' , of secret-keys.

FIGURE 6 illustrates computation of TLCK T , by originating or sending entity.

FIGURE 7 illustrates computation required for verification by receiving entity of TLCK from originating or sending entity.

FIGURE 8 illustrates computation of user-associated key.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a method and system for mutual authentication between two entities. Hereinafter, this specification will describe the present invention according to the preferred embodiments of the present invention. However, it is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned that those skilled in the art may devise various modifications and equivalents without departing from the scope of the appended claims.

General embodiment

The present invention discloses a method and system for computation and verification of authentication parameters between two entities. Reference is being made to FIGURE 1. FIGURE 1 illustrates a preferred embodiment of a method and system for computation and verification of authentication parameters between two entities. The two entities are an originating entity, being a server (100) or a client (110) and a receiving entity, being a server (100) or a client (110).

The server (100) component houses the application of the present invention and the client (110) component serves as an interface element for a particular human user (120) of interest. A trusted application or system (130) is installed on a computing device in the physical possession of aforesaid user which might be a desktop workstation or mobile device capable of localised computations of aforesaid server-associated Time or Location-Constrained Keys (TLCKs) as required by embodiment of interest; display of numeric, symbolic or graphical elements resulting from particular use of such embodiment; and communications with server for

management of keys used for computation of TLCKs as required on routine basis, such that aforesaid TLCKs can be associated with user of interest. The user-associated keys are subject to refreshment and replacement on periodic or episodic basis. Optionally, the method may
5 comprise image capture by means of camera attached to computing device on which trusted system (130) is installed.

An exemplary embodiment of the present invention would be a Web client-server system, in which service request is executed over the Internet to
10 server (100) of interest from client-side User Interface (UI) (110) as downloaded onto Web browser application on computing device of interest; following which TLCK associated with aforesaid server (100) is therein computed, and subsequently transmitted (101) to client UI (110); on which TLCK of interest is represented as numeric or symbolic string
15 (111) in a form and length suitable for human visual comparison (111A), or visual representation (112) in a form and function suitable for human visual comparisons and interactions (112A), or image encoding (113) in a form suitable for transfer (113A) to the trusted system (130), by means inclusive of image capture by means of camera on the trusted system
20 (130) or direct transfer as file of suitable encoded form to aforesaid trusted system (130).

Aforesaid embodiment furthermore enables user of interest (120) to undertake comparison against corresponding TLCK instance as computed
25 on the trusted system (130), outcome of which is deemed to be trustworthy by the user; and with aforesaid TLCK in representative form of numeric or symbolic string (111), with visual comparison of test values (111A) against reference values (131A); or in visual representation (132) with equivalent comparison of test interaction outcomes (112A) against
30 corresponding reference outcomes (132A).

Alternative embodiment enables aforesaid user (120) to entrust the trusted system (130) of interest to rigorously and unambiguously verify the authenticity and correct association of received TLCKs; in representative
5 form of numeric or symbolic string (111), with verification (131) following manual transcription (131A) onto aforesaid trusted system; or as image encoding (113) with an equivalent verification (133) following transfer (113A) as aforesaid.

10 Embodiment with visual interactive verification

Reference is now being made to FIGURE 2. FIGURE 2 illustrates an embodiment of the present invention with visual interactive verification. FIGURE 2 depicts a client UI component (210) with which to interact with
15 a particular user of interest (260), and a server component (200) in communication with aforesaid client component. The server (200) computes a server-associated TLCK T , in visual form constituting a test representation $X = X(T)$ (211), for subsequent display on aforesaid client component; and additionally a trusted application or system (250),
20 associated with aforesaid particular user, on which verification of aforesaid server-associated TLCK representation X (211) is undertaken by means of computation and display of reference representation $X' = X(T')$ (251), of corresponding T' independently measured or computed on trusted system, on aforesaid trusted system by means of correlated interactions (261 and
25 262), as respectively executed on client component and trusted system. This enables the determination (263) as to whether server-associated TLCK T is correct and correctly associated with server.

Visualisation and comparison of test valuation X (211) against reference
30 valuation X' (251) is undertaken by means of progressive and interactive

comparison (261) on client component, and correspondingly (262) on trusted system; such that user can undertake verification (263) of T in substantively greater detail than would be possible with any single truncation [T] into symbolic or numeric form, and of short length suitable
5 for human visual comprehension.

Visualisation as aforesaid is subject to progressive iteration $X.i = X(T; i)$: in $i = 1 \dots n$ steps subject to sequence of iterative interactions (212) by user, and progressive computations (213) for test valuation X associated with
10 server, and corresponding interactions (252) and consequent computations (253) for reference valuation X' on trusted system; subject to representation limit n as specified in representation method, and as corresponding to information content of TLCK input.

15 Embodiment as aforesaid then allows user to verify server-associated TLCK T as being authentic if corresponding representations X.i (211) and X'.i (251), subject to visual interactive comparison $V.i = V(X.i, X'.i)$ (263) as undertaken by user of interest at every step i. Embodiment then allows determination of T as authentic, arising from $T = T'$, if $V.i = \text{true}$ for all
20 progressive steps interactively undertaken by user; and conversely, determination of T as inauthentic, arising from $T \neq T'$; if $V.i = \text{false}$ for any step in sequence of interest.

Various embodiments of the present invention require prior association of
25 Public-Key Cryptography (PKC) pair (k, K) to server of interest, such that private-key k is securely and exclusively associated with server; and corresponding public-key K is likewise uniquely and unambiguously associated, and is furthermore available to trusted systems associated to all users of interest prior to commencement of any given interaction
30 executed by the embodiments of the present invention.

All users of interest are required to be associated with their respective key-pairs, such that a particular user i is equivalently associated with key-pair $(k.i, K.i)$, such that constituent private-key $k.i$ is likewise secure and
5 exclusive, on trusted system associated with user i , and corresponding public-key $K.i$ is likewise unique and unambiguous, and furthermore reciprocally available to server prior to any interaction of interest.

Embodiment with computer-assisted verification, with consequent
10 interaction-specific key

Reference is now being made to FIGURE 3. FIGURE 3 illustrates an embodiment of the present invention with computer-assisted verification, with consequent interaction-specific key. This embodiment allows
15 interaction sequence comprising computation of aforesaid TLCK T (302) by server (300) on request by particular user i (360), encoding (301) of TLCK T into machine-readable graphical form $Y = Y(T)$, by means of designated PKC computation, transmission (303) of Y , corresponding to particular service request to client UI component (310), and subsequent
20 display (311). Thereafter the method comprises transfer (312) of Y , upon designated action by user, by means of image capture of Y on computing device on which trusted system is installed, by means of camera attached to aforesaid device or direct transfer as file containing Y to aforesaid computing device. Following that the method comprises verification $W =$
25 $W(Y(T); K, k.i)$ (351) on trusted system (350), by means of another PKC computation; for determination (352) of TLCK T to be authentic if $W = \text{true}$, arising from $T = T'$, and furthermore if secret-key $k' = k'(K, k.i)$ (353) is unique to interaction of interest; and conversely for determination of TLCK to be inauthentic if $T \neq T'$ if $W = \text{false}$.

Various embodiments of the present invention require any user i of interest to have access to secret-key s associated with server; for subsequent computation by server, and verification by user i , of server-associated TLCKs; and as delivered to user i by means of secure-message $Z(K.i, s; k)$ as generated by server, and specifically designated for user i ; such that corresponding recovery $Z'(Z, K; k.i)$ requires correct demonstration of private-key $k.i$ by user i , as corresponds to public-key $K.i$ used in aforesaid computation of Z by server, and as previously associated with user i ; consequent to which session-key s is recovered by user i , and is verified to be correct and correctly associated with server.

These embodiments also require server to have reciprocal access to secret-key $s.i$ associated with user i ; for subsequent computation by user i , and verification by server, of user-associated TLCKs; and as delivered to server by means of reciprocal secure-message $Z(K, s; k.i)$ generated by user i , and specifically designated for server such that corresponding recovery $Z'(Z, K.i; k)$, and consequent verification of aforesaid secret-key $s.i$, requires correct demonstration and association reciprocal to aforesaid requirement.

20

Reference is now being made to FIGURE 4. FIGURE 4 illustrates computation Z and recovery Z' of cryptographic signatures or secure-messages. This comprises computation (410) by originating or sending entity (400) of secure-message (420) designated for receiving entity (450) with necessary inputs of receiver public-key (411) as previously associated, own private-key (412) as correctly demonstrated and secret-key (413) of interest to be protected within secure-message as subsequently transmitted and received by receiving entity previously designated as aforesaid. Thereafter, the method comprises undertaking corresponding computation for recovery (460) of previously received

30

secure-message with necessary inputs of own private-key (462) as correctly demonstrated and as corresponding to public-key (411) used by sending entity to compute secure-message of interest, and sender public-key (461) as also corresponding to private-key (412) used as aforesaid.

5 The outcome is such that receiving entity is able to recover secret-key (463) associated with sending entity as aforesaid, and furthermore to verify secret-key as correct and correctly associated.

Other embodiments of the present invention allows for user-associated $s.i$ to be established by means of PKC computation Z'' as executed

10 independently by server and user i , such that respective computations $Z''(K.i; k)$ by server allows computation of $s.i$, subject to verification of correctness and correct association; and $Z''(K; k.i)$ by user i allows equivalent computation of $s.i$, subject to equivalent verification; as well as

15 further requirement of correct demonstrations and associations as aforesaid.

Reference is now being made to FIGURE 5. FIGURE 5 illustrates independent establishment Z'' of secret-keys. This comprises interacting

20 entities (500 and 550) undertaking respective computations (510 and 560) independently of each other. The necessary inputs are other entity public-key (511) and own private-key (512), for first entity (500) of interest; and similarly other entity public-key (561) and own private-key (562), for second entity (550) of interest. Both entities (500 and 550) are engaged in

25 interaction (590) of interest, resulting in independent establishment (591 and 592) of common session-key. Additionally, each entity is able to undertake verification of aforesaid session-key as correct and correctly associated.

Various embodiments of the present invention would additionally require periodic or episodic execution of aforesaid key-generation by associated entity, and subsequent transport to other entity by means of secure-message; and key-establishment as independently computed by both
5 entities. This is subject to the requirements of the particular embodiment.

Technical specifications pertaining to mutual authentication sequence

Computation of server-associated TLCK

10

According to the preferred embodiment of the present invention, computation of server-associated TLCK allows server to compute associated TLCK T , and correspondingly trusted system associated with any user of interest to verify aforesaid TLCK. This is accomplished by
15 mean of secret-key s , as previously associated with server prior to any interaction of interest as aforesaid; and as additionally distributed to aforesaid trusted systems, likewise prior to any interaction.

According to the preferred embodiment of the present invention, the
20 method further undertakes computation of server-associated TLCK $T = T([t], [x], p; s)$ as the ZK integration of several inputs. One of these inputs comprises time t as measured from server system clock, with subsequent reduction $[t]$ to applicable resolution previously specified, and with equivalent reduction to be executed by other entity in subsequent
25 interaction of interest. Another input comprises location x as computed from information associated with incoming service request by user of interest, as might be inclusive of information obtained from system client, as might be inclusive of script or object operating within third-party application, as exemplified by Web browser or application previously
30 installed on computing device associated with user or request of interest;

such information inclusive of IP address associated with request of interest, or information pertaining to geographic location of system client, as exemplified by location-aware Web browser; with subsequent reduction [x] to applicable resolution previously specified, likewise with equivalent
5 reduction to be executed by other entity of interest. Other inputs include parameter p computed from and unique to service request of interest; and secret-key s previously associated to server as aforesaid.

Resultant server-associated TLCK T is then transmitted to client-side UI in
10 interaction of interest, in form of symbolic or numeric string [T] of length suitable for human visual comprehension; with subsequent manual transcription to trusted system associated to particular user of interest as aforesaid; or alternatively image capture and subsequent decoding resulting in recovery of [T] on trusted system of interest; or in form of
15 visual representation X(T) suitable for human interaction and visual comparison as aforesaid, with possibility of image capture and subsequent decoding to verify TCLK T on trusted system as aforesaid; or alternatively in form of graphical representation Y(T) in machine-readable form suitable for machine-to-machine transfer from client UI to trusted system of
20 interest; by means of image capture or image file receipt to recover T on trusted system as aforesaid.

Verification of server-associated TLCK

25 According to the preferred embodiment of the present invention, verification of aforesaid TLCK received from server as test valuation T is to be compared against one or more reference valuations T', as subsequently computed on trusted system associated with interacting users of interest.

Computation of reference $T' = T'([t'], [x'], p; s)$ on trusted system of interest is then executed on combination of inputs equivalent to inputs used in computation of corresponding test T to be verified. One of these inputs comprises time t' as measured from clock on trusted system, and
 5 subsequent reduction $[t']$ to applicable resolution previously specified, and furthermore equivalent to reduction previously executed by server in interaction of interest. Another input comprises location x' by means of information obtained from apparatus for measurement of location attached to trusted system, as exemplified by GPS radio; or systems or apparatus
 10 for determination of location arising from wireless communication network(s) to which trusted system is attached, such determination obtained from characteristics of local communications environment(s) of interest, as exemplified by WLAN or cellular radio; with subsequent equivalent reduction $[x']$ to applicable resolution previously specified, and
 15 furthermore equivalent to reduction previously executed by server. Other inputs include parameter p computed from and unique to service request of interest; and secret-key s previously associated to server as aforesaid, and furthermore accessible on trusted system prior to interaction of interest.

20

According to the preferred embodiment of the present invention, the method further undertakes additional computations of reference

$$T' = T'([t'] \pm c \cdot dt, [x'] \pm c' \cdot dx, y; s), \text{ in which:}$$

dt is granular unit of time resolution applicable to interaction of interest;

25 dx is granular unit of position resolution likewise applicable;

c is multiplier for units of time displacement deemed to be acceptable for verification of interest; and

c' is multiplier for units of position displacement likewise deemed to be acceptable.

30

Server-associated test valuation T , as received, is then deemed to be authentic or otherwise, as the case might be, subject to verification $Q(T, T')$ against one or more reference valuations of T' computed as aforesaid on trusted system of interest. TLCK T , as transmitted by server and received by trusted system; is deemed authentic with $Q(T, T') = \text{true}$, if $T = T'$ holds for one reference valuation computed as aforesaid during verification; or alternatively deemed inauthentic with $Q(T, T') = \text{false}$, if $T \neq T'$ for all reference valuations computed as aforesaid.

10 Computation of reciprocal user-associated TLCK

According to the preferred embodiment of the present invention; computation, on aforesaid trusted system associated with user i , of correspondingly associated reciprocal TLCK $T.i$, is subject to prior verification of received TLCK T as being correct and correctly associated with server. Such computation is by means of secret-key $s.i$; previously associated with particular user i of interest prior to any interaction of interest as aforesaid, and additionally distributed to server, likewise prior to any interaction; or alternatively secret-key unique to interaction of interest, as previously established to be correct and correctly associated.

The preferred embodiment of the present invention undertakes consequent computation of user-associated TLCK $T.i = T.i(T, [t'], [x'], p; s.i)$ from the ZK integration of several inputs. One of these inputs comprises received TLCK T , as previously verified to be correct and correctly associated with server. Other inputs comprise $[t']$ as reduction of time measurement, as used in aforesaid verification, and $[x']$ as reduction of position measurement or determination, similarly used as aforesaid. Further inputs comprise parameter p computed from and unique to service

request of interest; and secret-key s_i previously associated to user i as aforesaid.

Resultant user-associated TLCK T_i is furthermore subject to
5 representation as symbolic or numeric string truncated to length suitable for human visual comprehension on UI of trusted system of interest, manual transcription to client-side UI of server system on which service request of interest was previously initiated; and subsequent transmission to server, for consequent verification of T_i , by means of communications
10 network of interest.

Verification of reciprocal user-associated TLCK

According to the preferred embodiment of the present invention,
15 verification of aforesaid reciprocal TLCK received from particular user i of interest comprises comparison of test valuation T_i against one or more reference valuations T'_i , as subsequently computed on server from which user i is requesting service of interest.

20 Computation of reference $T'_i = T'_i(T, [t], [x], p; s_i)$ on server is then executed as ZK integration of inputs equivalent to inputs used in computation of corresponding test T_i to be verified. One of these inputs comprises TLCK T , as previously transmitted from server to particular user i of interest, and as presumed to be verified as correct and correctly
25 associated with server, as previously undertaken on trusted system associated with aforesaid user i . Other inputs comprise $[t]$ as reduction of time measurement, as used in computation of T'_i on aforesaid trusted system, and $[x]$ as reduction of position determination, as similarly used in aforesaid computation of interest. Further inputs comprise parameter p

computed from and unique to service request of interest; and secret-key $s.i$ previously associated to user i as aforesaid.

Primary embodiment of interest might additionally undertake additional
5 computations of reference

$T'.i = T'.i([t] \pm c.dt, [x] \pm c'.dx, y; s.i)$, in which:

dt is granular unit of time resolution applicable to interaction of interest;

dx is granular unit of position resolution likewise applicable;

c is multiplier for units of time displacement deemed to be acceptable for
10 verification of interest; and

c' is multiplier for units of position displacement likewise deemed to be acceptable.

User-associated test valuation $T.i$ as received, is then deemed to be
15 authentic or otherwise, as the case might be. This is subject to verification
 $Q'(T.i, T'.i)$ against one or more reference valuations of $T'.i$ computed as
aforesaid on server. TLCK $T.i$ transmitted by user i and received by server;
is deemed authentic, with $Q'(T.i, T'.i) = \text{true}$, if $T.i = T'.i$ holds for one
reference valuation computed as aforesaid during verification; or otherwise
20 deemed inauthentic, with $Q'(T.i, T'.i) = \text{false}$, if $T.i \neq T'.i$ for all reference
valuations computed as aforesaid.

Computation and verification of TLCKs

25 Reference is now being made to FIGURE 6. FIGURE 6 illustrates
computation of TLCK T by originating or sending entity. Computation (610)
of TLCK T (620) by sending entity (600) is accomplished by means of ZK
integration of several inputs. The inputs comprise secret-key s (611), as
previously associated with sending entity; transaction parameter p (612),
30 as optional input arising from interaction of interest; and received TLCK q

(613), as additional optional input computed by and associated with other entity of interest in aforesaid interaction. Other inputs comprise reduction [t] (624) of time t (614), as measured on entity of interest and subject to reduction computation (620) as previously specified for time inputs, and as
5 commonly executed on all interacting entities of interest. Further inputs comprise optional input reduction [x] (625) of location x (615); as also measured or otherwise determined on aforesaid entity, and as similarly subject to reduction computation (620) as equivalently specified for location inputs and likewise commonly executed. This results in TLCK
10 output (630) subsequently transmitted to other interacting entity.

Reference is now being made to FIGURE 7. FIGURE 7 illustrates computation required for verification by receiving entity of TLCK from originating or sending entity. Verification computation (710) by entity (700)
15 in receipt of TLCK from sending entity of interest is undertaken by means of ZK integration of several inputs. The inputs comprise received TLCK q (713) as aforesaid, to be regarded as test valuation in verification of interest; and secret-key s (711); as associated with sending entity, as accessible to receiving entity prior to interaction of interest, and
20 furthermore as presumed used in computation of received TLCK. Other inputs comprise transaction parameter p (712) as optional input arising from interaction of interest. Further inputs comprise reduction [t'] (724) of time t' (714); as measured on entity of interest, and subject to reduction computation (720) as previously specified for time inputs, and furthermore
25 as presumed executed in computation of received TLCK. Optional inputs comprise reduction [x'] (725) of location x' (715); as also measured or otherwise determined on aforesaid entity, and as similarly subject to reduction computation (720) as equivalently specified for location inputs, and likewise presumed executed for received TLCK. These aforesaid
30 reductions are subject to error toleration (730) inclusive of granularity dt

(734) of time reduction, and corresponding multiplier $c(t)$ (734A). This results in multiplicity of time valuations $[t'] \pm c(t).dt$. This error toleration is optionally inclusive of granularity dx' (735) of location reduction, and corresponding multiplier $c(x)$ (735A). This further results in multiplicity of location valuations $[x'] \pm c(x).dx$; with aforesaid time and location multiplicities resulting in multiplicity of reference TLCK valuations $q'(t', x') = q'([t'] \pm c(t).dt, [x'] \pm c(x).dx)$ (740). With this, the method undertakes comparison against received valuation q as received; and consequently results in determination $Q(q, q')$ (750) of received TLCK as being correct and correctly associated with sending entity, or otherwise as the case might be.

Technical requirements pertaining to key protection

Various embodiments of the present invention require association of secret-key or private-key as aforesaid to particular user of interest with consequent requirement for secure protection of constituent key-factors thereof on trusted system associated with particular user i . This is such that rigorous demonstration of key-factors is required for correct computation of secret-key or private-key. Consequently, this requires correct computation of interaction parameters as required for correct outcome in interaction of interest.

According to the preferred embodiment of the present invention, the method requires demonstration of all constituent key-factors x_i , for correct computation of secret or private-key $x = x(x_i: \text{for all } i = 1 \dots n)$. Such key-factors are possibly inclusive of secret password, as presumed known exclusively by particular user of interest; or furthermore one or more parameters, as presumed unique to computing device on which trusted system is installed. This is so that computation of x cannot be executed in

absence of any constituent key-factor x_i not correctly demonstrated; and furthermore that any compromise, to entity other than authentic user of interest, of one or more key-factors does not result in compromise of other key-factors, or consequent secret or private key.

5

Other embodiments of the present invention requires demonstration of specified plurality k from total of n key-factors for correct computation of secret or private-key $x = x(x_i: \text{for } i = k\text{-of-}n)$; as might be applicable for combination of secret password, as presumed exclusive to particular user as aforesaid; and one or more parameters as presumed unique to
10 respective computing device on which instance of trusted system is installed. This is such that computation of x can be executed to identical correct outcome, on multiple instances of trusted system installed on multiplicity of computing devices associated with particular user. This
15 comes with additional requirements that computation of x cannot be executed in absence of any constituent key-factor x_i not correctly demonstrated, and furthermore that compromise of one or more key-factors less than previously specified plurality $k\text{-of-}n$ does not result in compromise of other key-factors, or consequent secret-key or private key.

20

Technical requirements pertaining to computation of user-associated key

Reference is now being made to FIGURE 8. FIGURE 8 illustrates computation of user-associated key. Computation (830) of secret-key or
25 private key x (840), as previously specified and associated with particular user (810) on trusted system (800) likewise associated with aforesaid user, is undertaken as ZK integration of several inputs. These said inputs comprise key-factors x_i (821) for $i = 1..n' < n$ external to trusted system (800) of interest; also previously specified, as might be exemplified by
30 password or PIN presumed to be secret and exclusive to user (810) of

interest. These said inputs also comprise other key-factors x_i (822) for $i = 1 \dots n$ internal to trusted system (800); likewise previously specified, as might be exemplified by system or device parameters presumed unique and exclusive to trusted system (800). All key-factors are subject to factorisation condition $f(x_i: i = 1 \dots n)$ (820) applicable on aforesaid key-factors x_i (821 and 822); as might require correct demonstration of entire set of $x_i: i = 1 \dots n$ as previously specified; or alternatively plural set of $x_i: i = k\text{-of-}n$, for specified plurality threshold k . This might be required for single correct valuation of user-associated key arising from multiple instances of user-associated trusted system, each operating on different computing devices, as requirement for correct computation $x = x(f(x_i))$ (830) of key valuation x (840), as subsequently used in various other computations of interest as aforesaid. Such use is subject to non-exposure of valuation x external to trusted system; and furthermore non-compromise of valuation x arising from consequent outcome of such computations transmitted external to trusted system of interest.

System of server, client and trusted application or system

The system according to the embodiments of the present invention comprises a server as a computer system in client-server form, such that client and server constituent components engage in exchange of data, inclusive of the aforesaid authentication codes, by means of a data communications network, with IP networks being exemplary embodiments.

The client component is a computer application previously installed on computer system in use by human user, which might be in location physically removed from that of corresponding server component, with script, applet or application downloaded into a Web browser being exemplary embodiments. The user is deemed to have requested some

specified service by means of invoking user interface element on client component.

The client component is able to determine time, location and other
5 information circumstantial to service request necessary for computation of
authentication code as aforesaid; and is then able to display said
authentication code in numeric or symbolic form suitable for user visual
comprehension as aforesaid. The client component is also able to accept
10 input of reciprocal authentication code in such form suitable for user
manual transcription by means of suitable user interface element, with
keyboard or keypad being exemplary embodiments; and is then able to
transmit such reciprocal authentication code submitted by user to server
component by means of aforesaid communications network. The server
15 component is able to execute computations necessary for verification of
reciprocal authentication code as aforesaid.

The trusted system is a computer application, such that the trusted system
has been installed on computer system under the control of human user,
with mobile device or computer workstation being exemplary
20 embodiments. The trusted system is in location proximate to client
component of server as aforesaid; and is able to determine time, location
and other information circumstantial to service request by means
independent of such equivalent determinations as executed by server prior
to computation of authentication code. The user is desirous of verifying
25 authentication code previously received from server by means of invoking
user interface element on trusted system. The trusted system is able to
execute computations for one or more reference authentication codes; and
is able to display such reference codes in numeric or symbolic form
suitable for user visual comparison against test code as displayed on
30 client component as aforesaid. The user is able to determine from such

visual comparison whether server has authenticated its identity; and is desirous of undertaking computation of reciprocal authentication code to be transmitted to server by means of invoking user interface element on trusted system. The trusted system is able to accept input of numeric or symbolic parameter associated with service or transaction of interest, with
5 keyboard or keypad being exemplary embodiments; and is able to compute, and then display reciprocal authentication code in numeric or symbolic form suitable for user visual comprehension. The user is able to manually transcribe reciprocal code as displayed on trusted system into
10 client component by means of suitable user interface element, with keyboard or keypad being exemplary embodiments; or alternatively able to transcribe, by computerised means as aforesaid, reciprocal code into client component; with trusted system and client components being applications on the same computer system as exemplary embodiments.

15

The server further undertakes computation, on periodic or episodic basis, of secret-key to be used for subsequent computation of authentication codes by server, and verification thereafter by human user; with subsequent transmission to trusted system associated with particular user
20 with authentication by means of cryptographic signature or secure-message designated for aforesaid trusted system. This is such that recovery by designated trusted system of secret-key enables aforesaid user to subsequently undertake verification of authentication codes transmitted by server; as subject to demonstration of the correct key-
25 factors by particular user of interest, and furthermore to configuration within trusted system.

The trusted system further undertakes computation, on periodic or episodic basis, of secret-key to be used for subsequent computation of
30 authentication codes by trusted system on behalf of associated human

user, and verification thereafter by server. Subsequently, transmission of secret-key to server; with authentication by means of cryptographic signature or secure-message designated for server; so that server can subsequently undertake verification of authentication codes transmitted by

5 user of interest.

CLAIMS

1. Method for computation and verification of authentication parameters between two entities, an originating entity and a receiving entity, upon initiating an interaction by the originating entity, a server (100) or a client (110) initiating a service request over a communications network which will be received by the receiving entity, the client (110) or the server (110), wherein the method comprises
- 10 the client (110) authenticating the server (100) by visual comparison of an authentication code in numeric, symbolic or graphical form computed by the server (100) to a plurality of reference codes computed on a trusted application (130); and the server (100) authenticating the client (110) by manual transcription of an authentication code computed and displayed on the trusted application (130) and comparison of the test code to a plurality of reference codes computed on the server (100).
- 15
- 20 2. A method according to claim 1, wherein computation of the authentication code by the server (100) and the trusted application (130) is based on Zero-Knowledge (ZK) transformation which further comprises the transformation of one or more inputs inclusive but not limited to
- 25 key information which is securely managed and rigorously associated to either the server (100) or the client (110); service information derived from the service request or a subsequent grant;

- time or location information measured or inferentially computed independently by either the server (100) or the client (110); and subsequently
- an evaluation of authentication code received from either the server (100) or the client (110) based on computation of the plurality of reference codes based on predetermined approximation of time or location such that the authentication code is equal to one of the plurality of reference codes.
3. A method according to claim 2, wherein the trusted application (130) comprises an application operating on a mobile device or computer workstation that does not have connectivity to the communications network or a direct connectivity the server (100).
4. A method according to claim 2, comprising the time information measured or inferentially computed independently; further comprising measurement of a plurality of values by independently operated and calibrated system clocks capable of producing measurement values that differ; and if the difference exceeds a predetermined maximum degree, then authentication fails.
5. A method according to claim 4, further comprising the location information measured or inferentially computed independently; further comprising computations on Global Positioning System (GPS) signals as received by the trusted application (130), or alternatively communications parameters which comprises protocol identifiers associated with Internet access, including addresses associated with the service request initiated the client (110) and network connectivity, including addresses associated with access points for wireless access points and cellular base stations.

6. A method according to claim5, wherein computation of the authentication code by the server (100) or the trusted application (130) is based on Zero-Knowledge (ZK) integration which further
5 comprises the inputs of
key information associated to the originating entity; and
predetermined approximation of time or location measured independently on the originating entity.
- 10 7. A method according to claims 6, wherein verification of the authentication code by the server (100) and the trusted application (130) is undertaken as Zero-Knowledge (ZK) query which further comprises the inputs of
key information associated to the receiving entity;
15 predetermined approximation of time or location measured independently on the receiving entity; and
predetermined plurality of extrapolations of time or location based on the independent measurement on the originating entity.
- 20 8. A method according to claim6, wherein the method further comprises computation of a reciprocal authentication code that integrates additional inputs associated with service information including a received authentication code.
- 25 9. A method according to claim7, wherein the method further comprises verification of a reciprocal authentication code that integrates additional inputs associated with service information including a transmitted authentication code.

10. A method according to claim 7, wherein the authentication code is computed on the server (100) and received by the client (110) in numeric, symbolic or graphical form suitable for use by the client (110), comprising
- 5 Visual comprehension of the authentication code;
Manual transcription of the authentication code into the trusted application (130) by means of numeric, symbolic or graphical data entry;
Visual or computer-assisted comparison of the authentication code against the plurality of reference codes computed on the trusted application (130); and
10 Manual or computer-assisted determination as to whether the authentication code is authentic proof of the server (100) identity.
- 15
11. A method according to claim 10, wherein the authentication code is computed on the server (100) and received by the client (110) in numeric, symbolic or graphical form suitable for sequential application by the client (110), comprising
- 20 Request for generation of a corresponding verification code on the trusted application (130);
Visual comparison of the authentication code and the plurality of reference codes as computed on the trusted application (130) system; and
25 Manual or computer-assisted determination as to whether the authentication code is authentic proof of the server (100) identity.
- 30
12. A method according to claim 11, wherein the authentication code associated with the server (100) in visual or graphical form and

the corresponding verification code as computed on the trusted application (130) depends on progressive and interactive computation, wherein visual comparison of the authentication and the plurality of reference codes are executed as an iterative and interactive sequence.

13. A method according to claim 10, wherein the authentication code is computed on the server (100) and received by the client (110) in an image or graphical form suitable for use by the client (110), comprising

Transfer onto the trusted application (130) by means of a camera or an equivalent imaging device attached to a hardware platform on which the trusted application is operating or equivalent transfer of designated image or graphical data directly to the trusted application (130); and subsequently

Verification within the trusted application (130) of the received authentication code against the plurality of reference codes as computed; and

Indication to the user (120) as to whether the authentication code is authentic proof of the server (100) identity.

14. A method according to claim 13 in which a reciprocal authentication code is computed and transmitted, and furthermore upon acceptable determination of the server (100) authenticity in numeric or symbolic form suitable for use by the client (110), comprising

Manual or automatic transcription into the trusted application (130) by means of numeric or symbolic data entry of additional inputs associated with service information;

Visual comprehension of the reciprocal authentication code as computed on the trusted application (130);

Visual or computerised transcription of the reciprocal authentication code into the client interface component (110) by means of numeric or symbolic data entry;

Transmission of transcribed reciprocal authentication code to the server (100) by means of the communications network;

Automatic comparison of the received authentication code against the plurality of reference codes computed on the server (100); and

Automatic determination as to whether the authentication code is authentic proof of the user (120) commitment to the service of interest.

15. A method according to claim 9, wherein the computation and verification of the authentication code requires the originating entity and the receiving entity to be able to access a secret-key as used in symmetric-key cryptographic protocols, and the secret-key is exclusively and irrefutably associated to the originating entity.

16. A method according to claim 15, wherein the secret-key used for computation of the authentication code is associated to a key-pair as used in asymmetric-key cryptographic protocols, whereby a private-key of the key-pair is exclusively and irrefutably associated to the originating entity and a public-key of the key-pair is accessible to the receiving entity prior to initiating interactions.

17. A method according to claim 16, wherein the use of the secret key or the private-key by the originating entity or the receiving entity is subject to rigorous control necessitating Zero-Knowledge (ZK)

demonstration of at least one constituent key-factors associated to the originating entity, comprising

secret password that is known exclusively by the user (120);
or

5 numeric or symbolic parameters that is uniquely associated to the server (100) or the client (110).

18. A method according to claim 17, wherein the use of the secret or the private-key depends on Zero-Knowledge (ZK) demonstration
10 of a plurality of constituent key-factors, such plurality subject to configuration prior to initiating interactions.

19. A method according to claim 18, wherein the user (120) associated with a plurality of trusted applications (130) being utilised
15 for computation and verification of the authentication code comprises the user (120) being able to rigorously and irrefutably demonstrate access to the plurality of corresponding constituent key-factors.

20 20. A method according to claim 16, wherein the public-key associated with the server (100) is accessible to the user (120) prior to initiating interactions between the server (100) and the client (110).

25 21. A method according to claim 20, wherein the originating entity or the receiving entity computes a cryptographic secure-message as a Zero-Knowledge (ZK) integration which comprises the input of
secret-key to be further utilized for subsequent computations of authentication codes by the originating entity or the
30 receiving entity;

5 private-key, previously associated with the originating entity or the receiving entity, allowing the outcome of the computation to be unambiguously and irrefutably verified by a plurality of other entities in prior possession of the corresponding public-key to effect that the originating entity or the receiving entity is deemed to have undertaken associative commitment with respect to being associated with the secret-key.

10 22. A method according to claim 21, wherein the computation of a cryptographic secure-message as a Zero-Knowledge (ZK) integration which further comprises the input of public-key associated with the receiving entity as expressly specified by the originating entity such that verification of the outcome of the computation comprises the private-key
15 corresponding to such public-key, as previously utilised by the originating entity, to effect that recovery of the secret-key from the outcome parameter and consequent verification can only be undertaken by the receiving entity.

20 23. A method according to claim 22, wherein the computation of the cryptographic secure-message is by the server (100), with subsequent transmission to the trusted application (130) to enable consequent computation of the secret-key specific to the interaction, subject to correct demonstration on the trusted application (130) of
25 the private-key, and furthermore subject to equivalent computation independently undertaken on the server (100) in relation to the interaction.

30 24. A method according to claim 23, wherein the reciprocal authentication code is computed using the session-key specific to

the interaction as independently computed on the server (100) and the trusted application (130) engaged in the interaction.

25. A method according to claim 22, wherein the secret-key or the
5 public-key associated with the originating entity or the receiving
entity depends on computation of the cryptographic signature by a
trusted third-party (TTP) system, wherein
the trusted third-party (TTP) is deemed to be trustworthy; and
the trusted third-party (TTP) public-key is accessible to the
10 originating entity and the receiving entity prior to the
interaction.

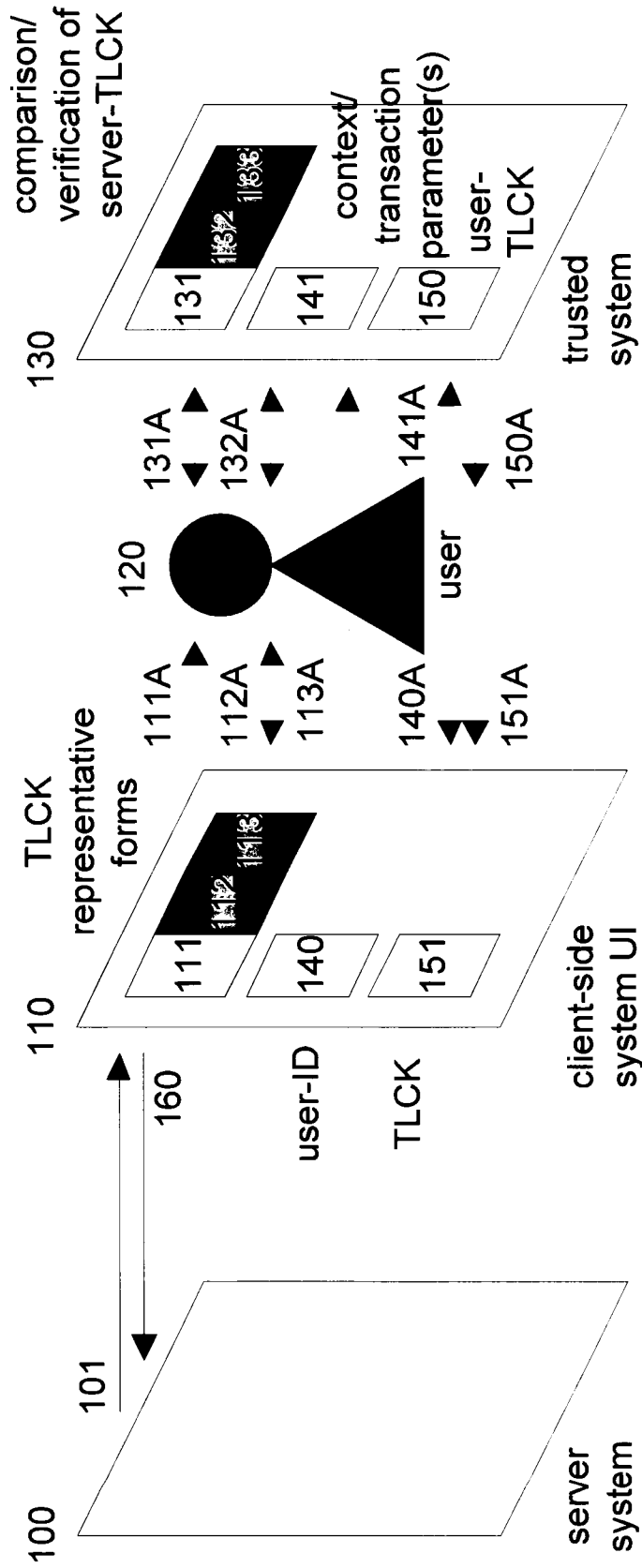


FIGURE 1

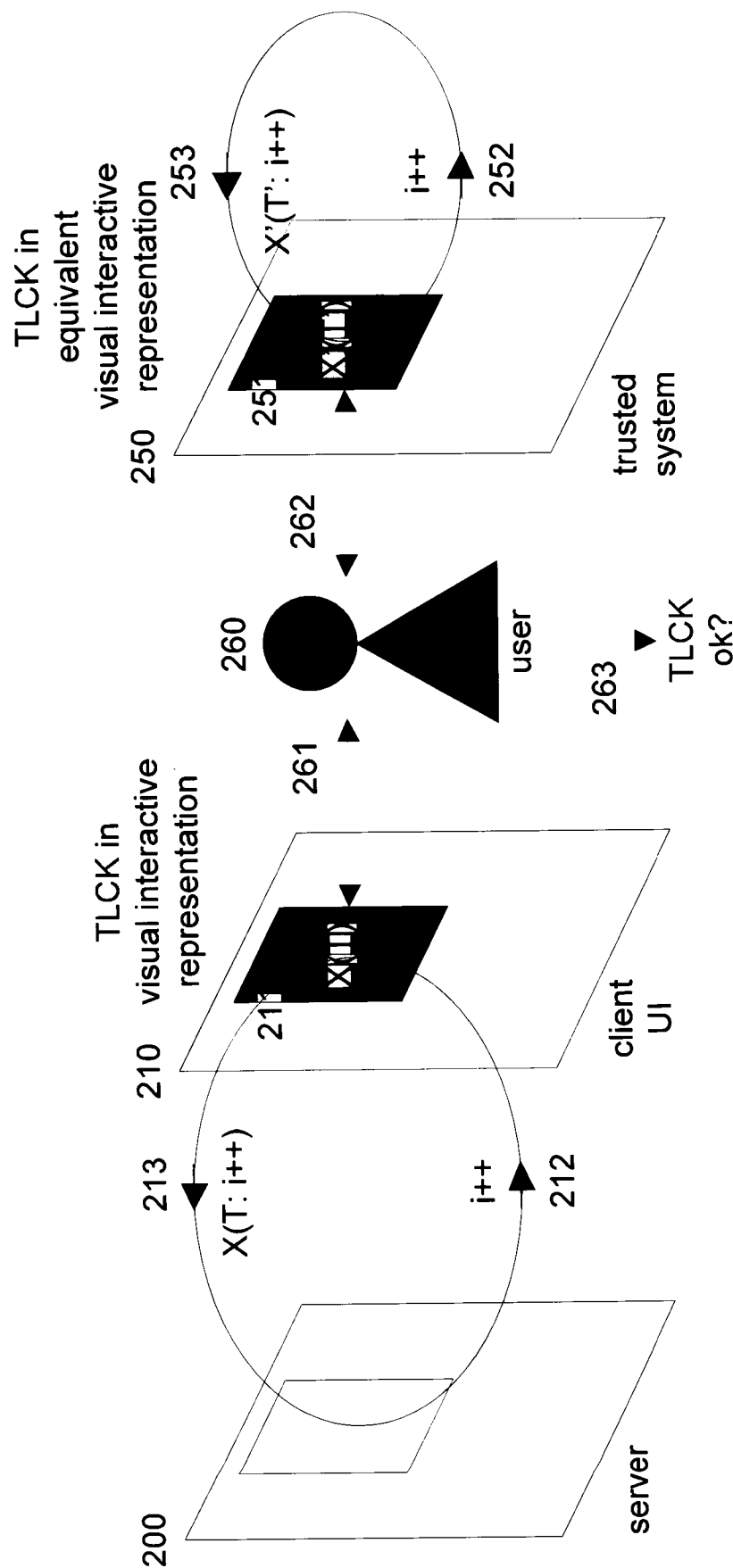


FIGURE 2

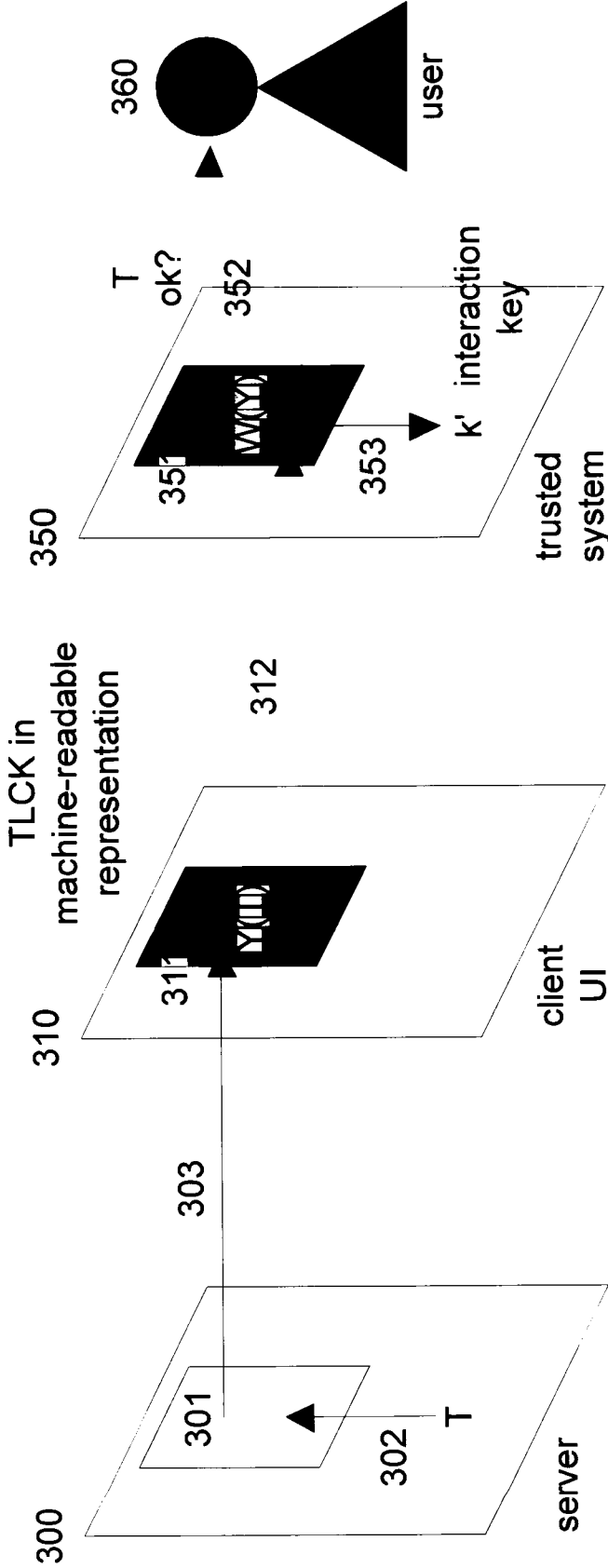


FIGURE 3

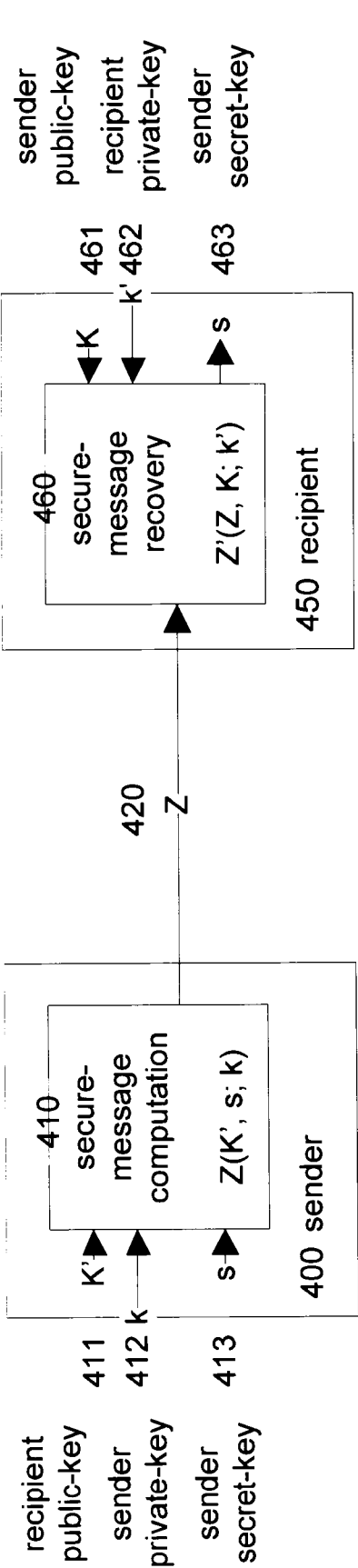


FIGURE 4

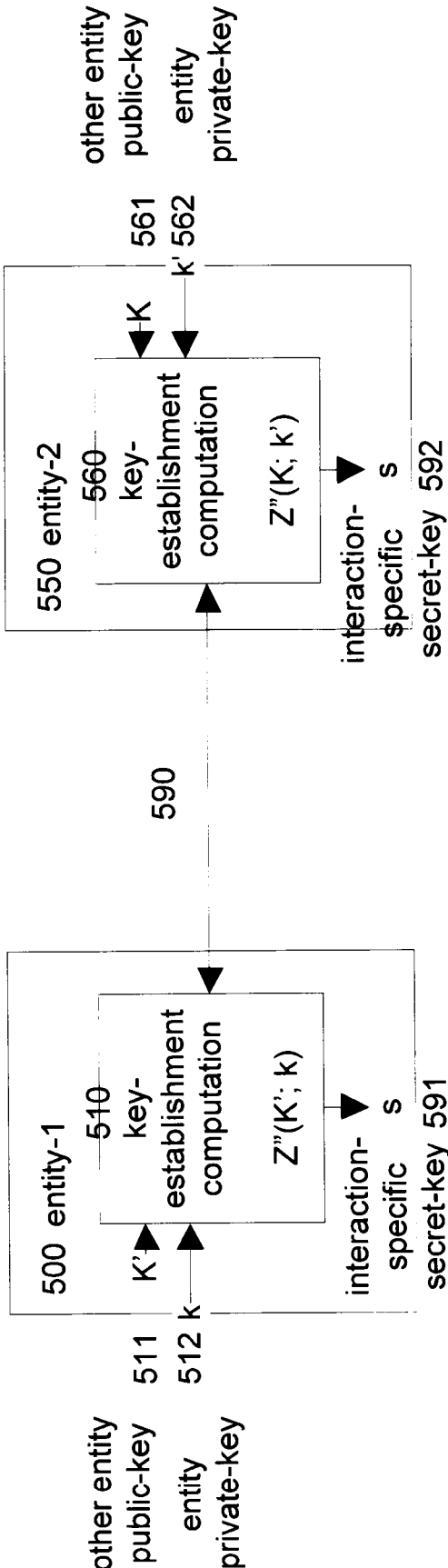


FIGURE 5

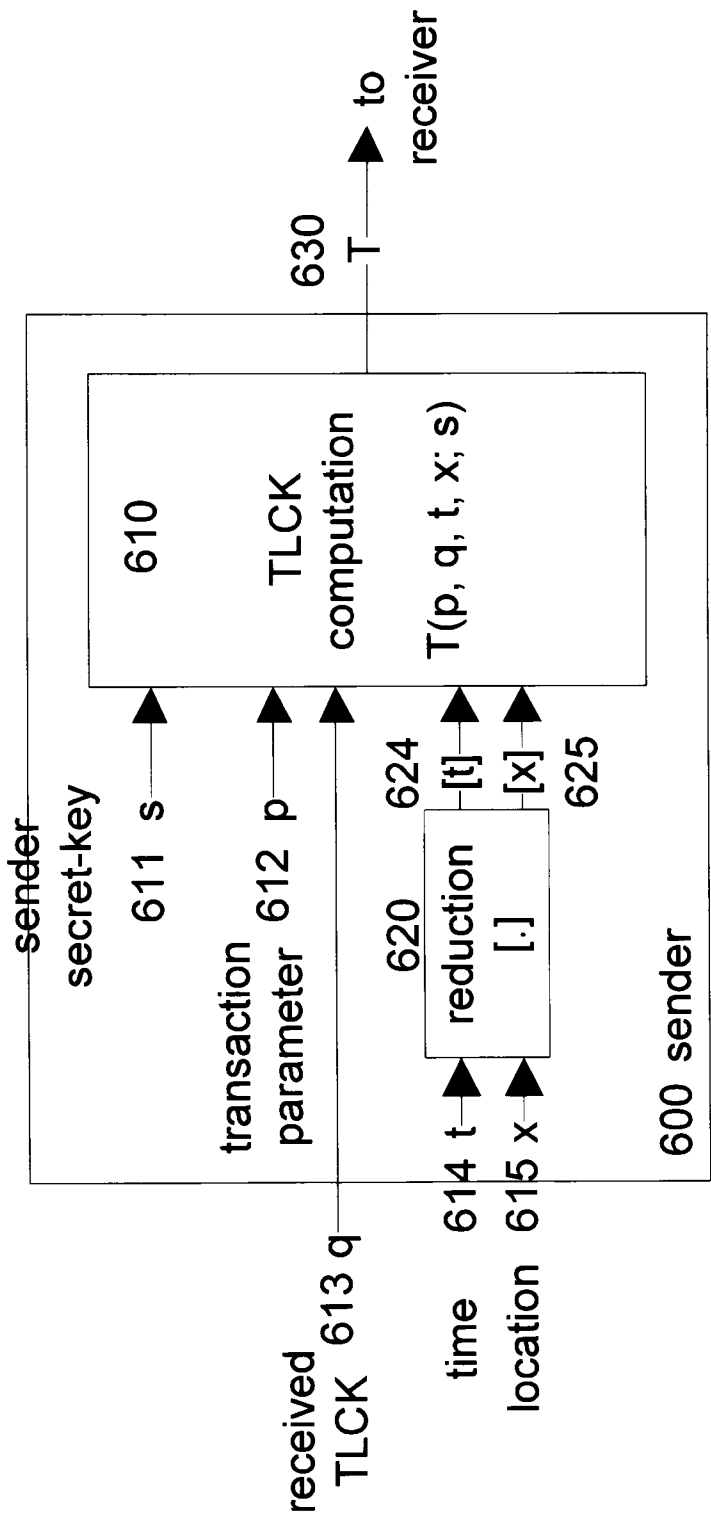


FIGURE 6

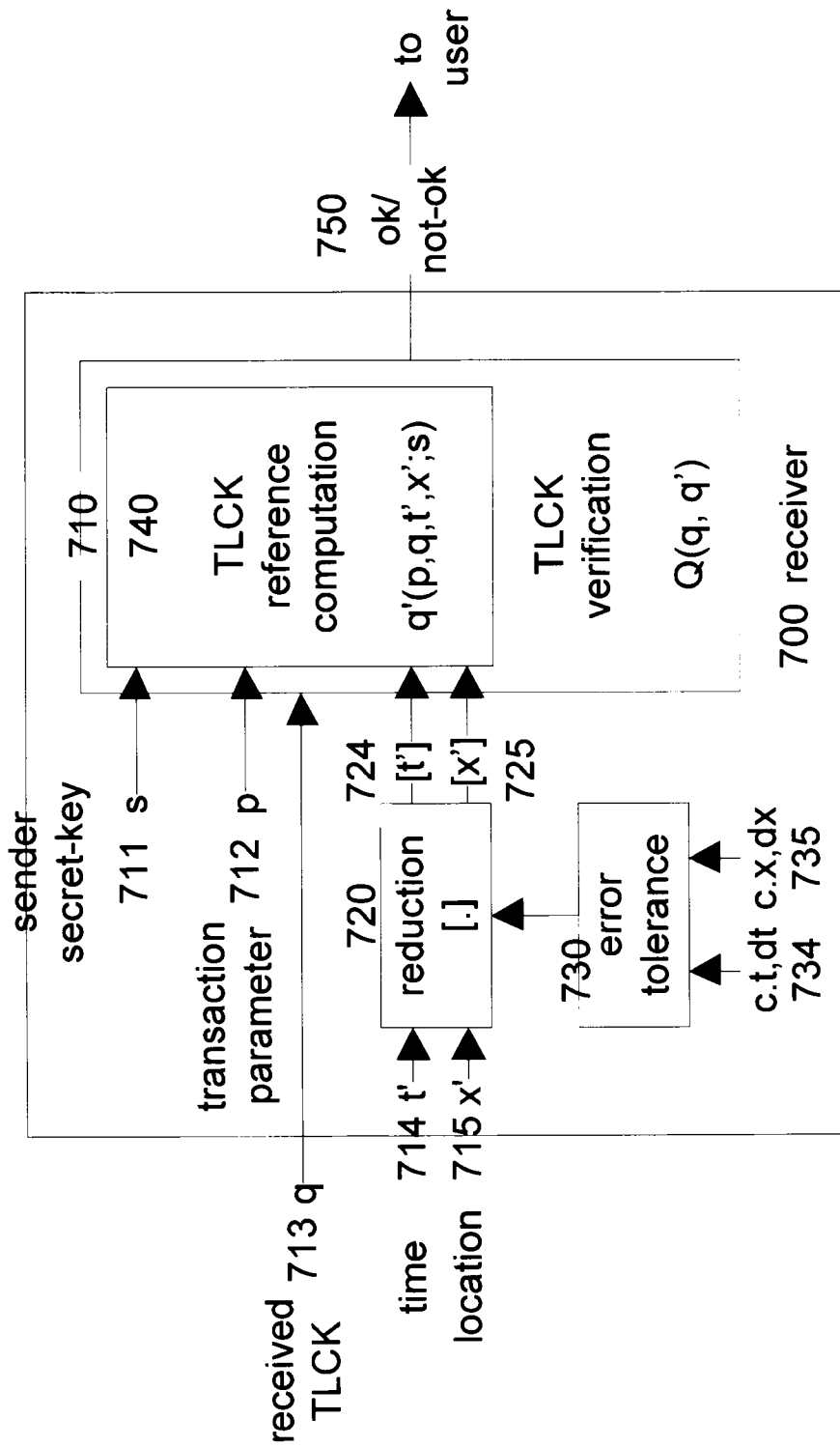


FIGURE 7

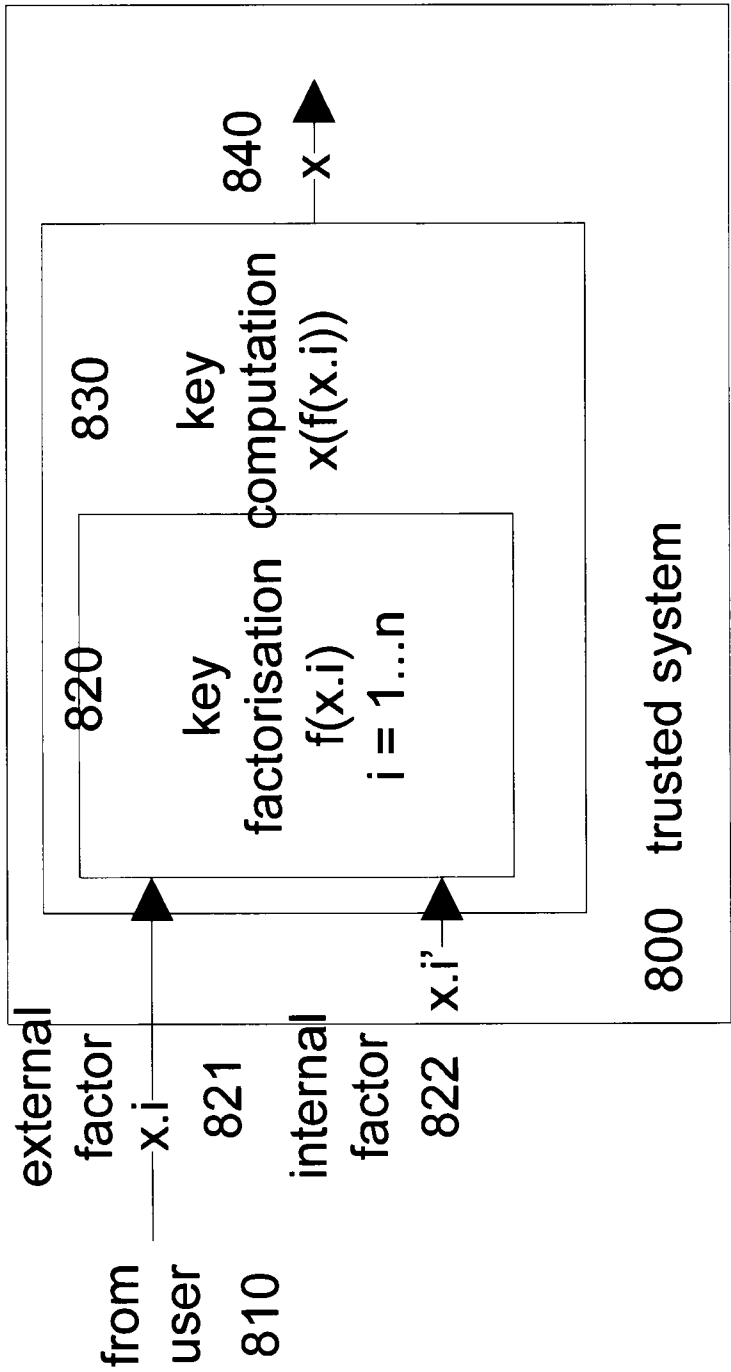


FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/000053**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/32(2006.01)i, H04L 9/08(2006.01)i**

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)

H04L 9/32; H04L 9/14; H04L 9/30; H04L 29/06; H04L 9/00; H04L 9/08

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: authentication, client, server, trusted application

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014-069985 A1 (MIMOS BERHAD) 08 May 2014 See page 9, line 11 - page 10, line 18; and figures 1, 3.	1
Y		2-25
Y	US 2010-0306531 A1 (HADI NAHARI) 02 December 2010 See paragraphs [0013], [0036]; and figure 1.	2-25
Y	US 2014-0189808 A1 (LOOKOUT, INC.) 03 July 2014 See paragraphs [0072]-[0092], [0128]; and figures 1-2B.	4-25
A	US 2010-0290618 A1 (GRZONKOWSKI SLAWOMIR et al.) 18 November 2010 See paragraphs [0030]-[0090]; and figures 3-5.	1-25
A	US 2007-0234041 A1 (SHREEKANTH LAKSHMESHVAR et al.) 04 October 2007 See paragraphs [0037]-[0067]; and figures 3-5.	1-25



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

14 December 2015 (14.12.2015)

Date of mailing of the international search report

15 December 2015 (15.12.2015)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM, Do Weon

Telephone No. +82-42-481-5560



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2015/000053

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014-069985 A1	08/05/2014	None	
US 2010-0306531 A1	02/12/2010	EP 2435963 A1	04/04/2012
		US 2010-0303230 A1	02/12/2010
		US 2010-0306076 A1	02/12/2010
		US 2010-0306107 A1	02/12/2010
		US 2010-0306819 A1	02/12/2010
		US 2015-288521 A1	08/10/2015
		US 8650614 B2	11/02/2014
		US 9135424 B2	15/09/2015
		WO 2010-138358 A1	02/12/2010
		WO 2010-138359 A1	02/12/2010
		WO 2010-138611 A1	02/12/2010
		WO 2010-138613 A1	02/12/2010
		WO 2010-138615 A1	02/12/2010
US 2014-0189808 A1	03/07/2014	GB 2523710 A	02/09/2015
		WO 2014-105263 A1	03/07/2014
US 2010-0290618 A1	18/11/2010	EP 2229750 A1	22/09/2010
		US 8411854 B2	02/04/2013
		WO 2009-083109 A1	09/07/2009
US 2007-0234041 A1	04/10/2007	AU 2007-231303 A1	04/10/2007
		BR PI0710257 A2	09/08/2011
		CN 101455053 A	10/06/2009
		CN 101455053 B	04/07/2012
		EP 2005702 A1	24/12/2008
		EP 2005702 A4	04/04/2012
		IL 194428 A	30/04/2012
		JP 2009-531764 A	03/09/2009
		JP 4824813 B2	30/11/2011
		KR 10-1038064 B1	01/06/2011
		KR 10-2008-0106982 A	09/12/2008
		MX 2008012363 A	09/10/2008
		MY 149495 A	13/09/2013
		RU 2008141089 A	10/05/2010
		RU 2414086 C2	10/03/2011
		US 8522025 B2	27/08/2013
		WO 2007-110468 A1	04/10/2007
		ZA 200809137 A	25/11/2009