(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 551 149 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 56
Description Paragraph(s) 8
Claims EN 8, 10, 12, 30
Numerous spelling errors of minor importance

(48) Corrigendum issued on:
10.10.2012 Bulletin 2012/41

(45) Date of publication and mention of the grant of the patent:
09.05.2012 Bulletin 2012/19

(21) Application number: **04293090.9**

(22) Date of filing: **22.12.2004**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(54) **Universal secure messaging for remote security tokens**

Universeller sicherer Datenaustausch für enfernte Sicherheitstoken

Transmission de messages sécurisée universelle pour les jetons de sécurité à distance

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR

(30) Priority: **22.12.2003 US 740920**

(43) Date of publication of application:
06.07.2005 Bulletin 2005/27

(73) Proprietor: **Activcard Inc.**
Fremont, CA 94555 (US)

(72) Inventors:
- **Wen, Wu**
  Sunnyvale
  CA 94087 (US)
- **Le Saint, Eric F.**
  Los Altos
  CA 94024 (US)
- **Becquart, Jérome Antoine Marie**
  Fremont
  CA 94536 (US)

(74) Representative: **Patentanwälte Freischem**
Salierring 47-53
50677 Köln (DE)

(56) References cited:
EP-A2- 0 733 971 **EP-A2- 0 957 651**
US-A- 4 993 068

- **DEUTSCHE TELEKOM AG: 'Das TeleSec LineCrypt L für sichere Netzwerkverbindungen' LINECRYPT L BENUTZERHANDBUCH, XX, XX 14 April 2000, pages 5 - 39, XP002207127**

EP 1 551 149 B9

Description

FIELD OF INVENTION

[0001] The present invention relates generally to a data processing system, method and computer program product and more specifically to a secure end-to-end wireless communications connection between a security token enabled computer system and an intelligent remote device having a security token operatively coupled thereto.

BACKGROUND

[0002] In high security operating environments, the US National Institute of Standards and Technology (NIST) specifies in FIPS PUB 140-2, "Security Requirements For Security tokens," for security levels 3 and 4 that critical security parameters (CSP) such as authentication data, passwords, PINs, CSPs, biometric samples, secret and private cryptographic keys be entered into or output from a security token in an encrypted form, generally using some form of physical and/or logical trusted path or secure messaging channel to prevent interception of the critical security parameters.

[0003] The security tokens referred to in this specification include hardware based security devices such as cryptographic modules, smart cards, integrated circuit chip cards, portable data carriers (PDC), personal security devices (PSD), subscriber identification modules (SIM), wireless identification modules (WIM), USB token dongles, identification tokens, secure application modules (SAM), hardware security modules (HSM), secure multi-media token (SMMC), trusted platform competing alliance chips (TPCA) and like devices.

[0004] The document XP 002207127 by Deutsche Telekom AG : Das TeleSecLine Crypt L für sichere Netzwerkverbindugen" describes a system offering a protected data transfer over Ethernet-based 2P networks.

[0005] The document EP-A-0733971 describes a method for managing connections between objects in a distributed object system.

[0006] Attempts at providing a physical trusted path include the use of cryptographic hardware devices installed between input devices such as the keyboard and possibly the mouse. An example of such a cryptographic interface device is disclosed in US Patent 5,841,868 to Helbig. However, the hardware expenditures and added administrative burden greatly increases the cost of the computer system.

[0007] In another approach, US patent 4,945,468 to Carson, et al., a trusted path is generated by providing a new virtual terminal window which allows secure entry of CSPs. The new virtual terminal window is effectively isolated from other running processes. This method is a reasonably secure approach but does not extend the trusted path to peripheral security devices such as cryptography modules, security tokens and biometric scanners.

[0008] In yet another approach, the document US 2002/0095587 A1 to Doyle, et al. discloses a wireless SSL or equivalent connection which utilizes negotiated time-limited cryptography keys to maintain a chain of trust between interconnected security devices. However, the mechanism disclosed relies heavily on multiple public key cryptography key pairs which is difficult to maintain and may reduce overall performance due to relatively slow transaction processing when employed using a smart card. In addition, negotiation of time-limited cryptography keys relies on devices containing a system clock for changing of cryptographic keys. Smart cards and like devices do not include system clocks and thus are reliant of their host for providing event timing which may introduce security concerns when the host is not trusted.

[0009] Cryptographic mechanisms are available in the relevant art which could be adapted to encrypt an incoming CSP with a cryptographic key for secure transport through a security token enabled and eventual decryption by a security executive installed within the security token. However, the cryptographic mechanism employed by the security token enabled computer system must provide a sufficient level of security to prevent interception of the cryptographic keys used in encrypting the CSP and furthermore limits vulnerability to a replay type attack.

[0010] Another common vulnerability in the relevant art relates to the lack of ability to bind a CSP to a session, which potentially allows an unlocked security token to be accessed by an unauthorized entity. To address this potential vulnerability, the CSP is typically cached or stored and presented by software to the security token each time access is required. The cached or stored CSPs are likewise vulnerable to interception or compromise by an unauthorized entity. Therefore, it would be highly advantageous to provide a secure CSP transport system which limits an intruder's ability to intercept a cryptographic key during wireless communications sessions, is relatively invulnerable to a replay type attack, minimizes requests for user input of CSPs already provided within a session and does not store or otherwise cache a CSP.

SUMMARY

[0011] With this goal in mind, the present invention is a method for establishing a secure end-to-end communications connection according to claim 1, a corresponding system according to claim 20 and a computer program product according to claim 43.

[0012] Other features of the invention are found in the dependent claims.

[0013] This invention addresses the limitations described above and provides an efficient secure end-to-end communications connection to securely exchange information between a security token enabled computer system and an intelligent remote device having a security

token operatively coupled thereto. The method portion of the invention comprises the steps of performing a first security transaction which authenticates a security token to a security token enabled computer system, establishing a secure communications connection between the security token and the security token enabled computer system which incorporates a shared symmetric key set generated during the first security transaction, assigning at least one key from the shared symmetric key set to a dedicated communications channel accessible to the security token, and performing a second security transaction which authenticates a user to said security token.

[0014] Steps are performed for signaling an affirmative result to the security token enabled computer system if the second security transaction is successful. The second security state is required before the secure communications connection is available for use by said security token.

[0015] The first security transaction is accomplished using a challenge/response protocol which incorporates an asymmetric key pair. A challenge is generated by the security token enabled computer system and encrypted with the public key associated with the security token.

[0016] The encrypted challenge is then sent to the security token. The security token decrypts the challenge using the private key counterpart to the public key and returns the clear text challenge to the security token enabled computer system for verification.

[0017] The public key is transferred to the security token enabled computer system by way of a digital certificate as part of the establishing the wireless communications connection.

[0018] The second security transaction authenticates the user to the security token by the user's critical security parameter which is provided directly or indirectly to the security token via the intelligent remote device. Once the second security transaction has been successfully completed the user is allowed access to one or more secure resources associated with the security token, security token enabled computer system or both.

[0019] In related embodiments of the invention, security states are maintained by the security token and security token enabled computer system. The security states are set by the successful completion of the first and second security transactions.

[0020] The secure communications connection is established by generating on the security token enabled computer system, a shared symmetric key set, encrypting one of the generated symmetric keys with the public key, sending the encrypted symmetric key to the security token, decrypting the symmetric key with the counterpart private key and assigning the decrypted symmetric key to a dedicated communications channel. The dedicated communications channel prevents the number of wireless secure communications connections with the security token from exceeding a predetermined limit. The predetermined limit is usually set to 1.

[0021] In another embodiment of the invention, user feedback is provided by the intelligent remote device which prompts the user to select either a local or remote authentication transaction and provide the critical security parameter.

[0022] In another embodiment of the invention authentication of the user is inhibited if outside a predefined range of a proximity sensor coupled to the security token enabled computer system.

[0023] In yet another embodiment of the invention, user sensory feedback is provided by the security token enabled computer system which indicates a remote authentication transaction is in progress. The user sensory feedback includes visual, tactile, aural or vibratory feedback.

[0024] A first systematic embodiment of the invention comprises a security token enabled computer system in wireless communications with an intelligent remote device having an operatively coupled security token thereto. The security token enabled computer systems includes a first security transaction means for at least authenticating the security token to the security token enabled computer system, and a first secure communications connection means for at least establishing a cryptographically encoded link between the security token enabled computer system and the security token. The first security transaction means includes a challenge/response protocol means and an asymmetric cryptography means. The first secure communications connection means includes a symmetric key set generation means and a secure symmetric key exchange means.

[0025] The security token enabled computer system further includes a first secure access means for allowing a user access to one or more secure resources following a receipt of an affirmative signal.

[0026] Successful execution of the first security transaction means sets a first computer system security state and receipt of the affirmative result signaling sets a second computer system security state associated with the security token enabled computer system.

[0027] The intelligent remote device includes a security token interface means for at least operatively coupling the security token to the intelligent remote device, and a user interface means for at least receiving and routing a critical security parameter provided by the user to the security token interface means. The user interface means includes conditional means for conditionally receiving the critical security parameter. The conditional means is intended to limit or prevent receiving the critical security parameter until the cryptographically encoded link is established. The security token interface means includes security token communications means and electromagnetic power transfer means.

[0028] The security token includes a secure communications connection means for at least establishing the cryptographically encoded link in conjunction with the first secure communications connection means, a dedicated communications channel means for preventing a concurrent cryptographically encoded link from being estab-

lished with the security token, a second security transaction means for at least authenticating the user to the security token using at least the critical security parameter and an affirmative signaling means for sending an affirmative signal to the security token enabled computer system following a successful completion of the second security transactions means. In an embodiment of the invention, the dedicated communications channel means includes a unique channel identifier means which is addressable by the security token enabled computer system.

[0029] In a related embodiment of the invention, establishment of the cryptographically encoded link sets a first token security state and successful execution of the second security transaction means sets a second token security state. In a related embodiment of the invention, the second security state is required before the secure communications connection is available for use by the security token.

[0030] A second systematic embodiment of the invention comprises a security token enabled computer system in processing communications with an intelligent remote device and a security token coupled to the intelligent remote device. The security token enabled computer system includes a first processor, a first memory coupled to the first processor, at least one remote authentication application operatively stored in a first portion of the first memory having logical instructions executable by the first processor to authenticate the security token, establish a secure end-to-end communications connection with the security token and allow a user access to one or more secure resources following a receipt of an affirmative signal sent from the security token.

[0031] The security token enabled computer system further includes a first wireless transceiver functionally coupled to the first processor and a public key associated with the security token retrievably stored in a second portion of the first memory.

[0032] The at least one remote authentication application further includes logical instructions executable by the first processor to generate a symmetric key set and perform a secure key exchange with the security token.

[0033] The intelligent remote device includes a second processor, a second memory coupled to the second processor, a security token interface coupled to the second processor, a user interface coupled to the second processor and at least one remote device interface application operatively stored in a portion of the second memory. The at least one remote device interface application includes logical instructions executable by the second processor to emulate a security token device interface locally coupled to at least the security token enabled computer system and conditionally receive and route a critical security parameter provided by the user via the user interface to the security token. The intelligent remote device further includes a second wireless transceiver functionally coupled to the second processor.

[0034] The communications and electromagnetic power interface includes inductive means, capacitive means or electric contact means to operatively couple the security token to the intelligent remote device. The at least one remote device interface application further includes logical instructions executable by the second processor to prevent receiving the critical security parameter from the user before establishment of the secure end-to-end communications connection.

[0035] The security token includes at least a third processor, a third memory coupled to the at least a third processor, a communications and electromagnetic power interface coupled to the at least a third processor and the security token interface and at least one token remote authentication application operatively stored in a first portion of the third memory.

[0036] The at least one token remote authentication application includes logical instructions executable by the at least a third processor to establish the secure end-to-end communications connection in conjunction with the security token enabled computer system, restrict the secure end-to-end communications connection to a single wireless secure communications connection, authenticate the user and send the affirmative signal to the security token enabled computer system ,if the user is successfully authenticated. The security token further includes an private key retrievably stored in a second portion of the third memory and a reference critical security parameter retrievably stored in a third portion of the third memory. The private key is the counterpart to the public key. The user is authenticated by the at least one token remote authentication application by comparing the user's provided critical security parameter to the reference critical security parameter.

[0037] The restriction to the secure end-to-end communications connection is applied to a dedicated communications channel controlled by the at least one token remote authentication application. The dedicated communications channel includes a unique identifier addressable by the security token enabled computer system.

[0038] The public and private keys are incorporated into a challenge/response protocol used to authenticate the security token to the security token enabled computer system and are further used to perform a secure symmetric key exchange from the security token enabled computer system to the security token.

[0039] In another embodiment of the invention, a proximity sensor is coupled to the security token enabled computer system which inhibits either authentication or use of the secure communications channel if the security token is outside of a predefined range from the security token enabled computer system.

[0040] In a final embodiment of the invention, a computer program product is provided. The computer program product is embodied in a tangible form readable by a security token processor and includes executable instructions stored thereon for causing the security token processor to utilize one or more security token emulation

services provided by an intelligent remote device processor, establish a secure end-to-end communications connection in conjunction with a security token enabled computer system processor, restrict the secure end-to-end communications connection to a single wireless secure communications connection, authenticate a user and send an affirmative signal to the security token enabled computer system processor if the user is successfully authenticated.

[0041] The computer program product further includes executable instructions stored thereon for causing the security token enabled computer system processor to authenticate the security token, establish the secure end-to-end communications connection with the security token, and allow a user access to one or more secure resources following a receipt of the affirmative signal sent from the security token.

[0042] The computer program product further includes executable instructions stored thereon for causing the intelligent remote device processor to provide the one or more security token emulation services to the security token processor, and receive and route a critical security parameter provided by the user via the user interface to the security token.

[0043] The tangible form of the computer program product includes magnetic media, optical media or logical media stored in a code format comprising byte code, compiled, interpreted, compilable and interpretable.

BRIEF DESCRIPTION OF DRAWINGS

[0044] The features and advantages of the invention will become apparent from the following detailed description when considered in conjunction with the accompanying drawings. Where possible, the same reference numerals and characters are used to denote like features, elements, components or portions of the invention. It is intended that changes and modifications can be made to the described embodiment without departing from the true scope and spirit of the subject invention as defined by the claims.

FIG. 1 - is a generalized block diagram of a security token enabled computer system.

FIG. 1A - is a generalized block diagram of an intelligent remote device.

FIG. 1B - is a generalized block diagram of a security token

FIG. 2 - is a detailed block diagram of one embodiment of the invention where a security token enabled computer system is in processing communications with a security token equipped intelligent remote device over a wireless link.

FIG. 2A - is a detailed block diagram of the invention where an public key is transferred to the security token enabled computer system.

FIG. 2B - is a detailed block diagram of the invention where the security token receives an encrypted challenge generated by the security token enabled computer system as an initial part of an authentication challenge/response protocol.

FIG. 2C - is a detailed block diagram of the invention where the security token returns the clear text challenge to the security token enabled computer system as a final part of the authentication challenge/response protocol.

FIG. 2D - is a detailed block diagram of the invention where a symmetric key set is generated and a secure key exchange is performed between the security token enabled computer system and the security token.

FIG. 2E - is a detailed block diagram of the invention where a secure end-to-end communications connection is established between the security token enabled computer system and the security token.

FIG. 2F - is a detailed block diagram of the invention where a user's critical security parameter is provided to the intelligent remote device and routed to the operatively coupled security token to authenticate the user.

FIG. 2G - is a detailed block diagram of the invention where the intelligent remote device has successfully been authenticated to the security token enabled computer system.

FIG. 3 - is a flow diagram illustrating the major steps associated with establishing the secure end-to-end communications connection between the security token enabled computer system and an intelligent remote device having a security token operatively coupled thereto.

DETAILED DESCRIPTION

[0045] This present invention provides an anonymous secure end-to-end communications connection which allows an intelligent remote device to emulate a locally connected security token device without requiring an actual physical connection to a security token enabled computer system. The anonymous secure end-to-end communications connection is established over a wireless communications network or link. The applications are envisioned to be programmed in a high level language using such as Java ™, C++, C #, C or Visual Basic ™.

[0046] Referring to Figure 1, a block diagram of a security token enabled computer system 105 is depicted.

[0047] The security token enabled computer system 105 includes a processor 5c, a main memory 10c, a display 20c electrically coupled to a display interface 15c, a secondary memory subsystem 25c electrically coupled to a hard disk drive 30c, a removable storage drive 35c electrically coupled to a removable storage unit 40c and an auxiliary removable storage interface 45 electrically coupled to an auxiliary removable storage unit 50c.

[0048] A communications interface 55c subsystem is coupled to a wireless transceiver 60c and a wireless network or link 65, an optional security token 75 electrically

coupled to a security token interface 70c and a user input interface 80c including a mouse and a keyboard 85, an optional biometric scanner 95c electrically coupled to an optional biometric scanner interface 90c and an optional proximity sensor 115c coupled to the communications interface 55c. The proximity sensor 115c prohibits remote authentications to be performed when a security token 75r (Figure 1A) is not within either a predefined distance from the proximity sensor 115c or within sensor range of the proximity sensor 115c. An example of suitable proximity systems adaptable for use in the invention is available from Ensure Technologies (Xyloc), 3526 West Liberty Road, Suite 100, Ann Arbor, Michigan 48103; www.ensuretech.com. The technical bases for the Xyloc proximity detection systems are disclosed in US patents and patent applications US 6,456,958, US 6,307,471, US 6,070,240, US 20020104012A1, US 20020069030A1, US 20020065625 all assigned to Ensure Technologies.

[0049] The processor 5c, main memory 10c, display interface 15c secondary memory subsystem 25c and communications interface system 55c are electrically coupled to a communications infrastructure 100c. The security token enabled computer system 105 includes an operating system, at least one remote authentication application, other applications software, cryptography software capable of performing symmetric and asymmetric cryptographic functions, secure messaging software and device interface software.Referring to Figure 1A, a block diagram of an intelligent remote device 110 is depicted. The an intelligent remote device 110 includes a processor 5r, a main memory 10r, a display 20r electrically coupled to a display interface 15r, a secondary memory subsystem 25r electrically coupled to an optional hard disk drive 30r, a virtual storage drive 35r and a removable memory module 50r electrically coupled to a removable memory module interface 45r.

[0050] A communications interface 55r subsystem is coupled to a wireless transceiver 60r and a wireless network or link 65, a security token 75 electrically coupled to a security token interface 70r and a user input interface 80r including a mouse and a keyboard 85r, and an optional biometric scanner 95r electrically coupled to an optional biometric scanner interface 90r.

[0051] The processor 5r, main memory 10r, display interface 15r secondary memory subsystem 25r and communications interface system 55r are electrically coupled to a communications infrastructure 100r. The intelligent remote device includes an operating system, at least one remote device interface application, other applications software, cryptography software capable of performing symmetric and asymmetric cryptographic functions, secure messaging software and device interface software.

[0052] Referring to Figure 1B, a block diagram of the security token 75 is depicted. The security token 75 includes a wireless, optical and/or electrical connection means 60t, 60w compatible with the security token interfaces 70c, 70r, a processor 5t, an optional cryptographic co-processor 5tc coupled to the processor 5t, volatile memory 10vm, non-volatile memory 10nvm, an electrically erasable programmable read only memory (EEPROM) 10eeprom and a communications interface 55t coupled to the connection means 60t.

[0053] The processor 5t, optional cryptographic co-processor 5tc, volatile memory 10vm, non-volatile memory 10nvm, electrically erasable programmable read only memory (EEPROM) 10eeprom and communications interface 55t are electrically coupled to a communications infrastructure 100t. The EEPROM further includes a runtime operating environment, cryptography extensions incorporated into the operating system and capable of performing symmetric and asymmetric cryptographic functions compatible with the intelligent remote device and security token enabled cryptography software, at least one token remote authentication application, one or more critical security parameter protected secure resources coupled to the at least one token remote authentication application and a public key infrastructure (PKI) key pair functionally coupled to the at least one token remote authentication application.

[0054] The non-volatile memory 10nvm has operatively stored therein one or more reference critical security parameters which are verified against a user supplied critical security parameter by the at least one token remote authentication application to allow access to the one or more one or more critical security parameter protected secure resources.

[0055] Referring to Figure 2, a generalized arrangement of the invention is depicted. The invention includes an intelligent remote device IRD 110 in processing communications over a wireless link 65 with a security token enabled computer system 105. A security token ST 75 is operatively coupled to the intelligent remote device IRD 110 via a security token interface device STI 70r.

[0056] The intelligent remote device IRD 110 includes an operatively coupled wireless transceiver T/R2 60r, a security token interface STI 70r, a user input means UI 85 and a display DI 202r which provides a user with information related to available authentication options and authentication status.

[0057] The security token interface STI 70r includes optical, capacitive, inductive and direct electrical contact type interface devices and provides electromagnetic power and communications continuity with the intelligent remote device IRD 110. Lastly, at least one remote device interface application RDI 210 is installed in the intelligent remote device IRD 110.

[0058] The at least one remote device interface application RDI 210 is generally a middleware application which allows the intelligent remote device IRD 110 to emulate a local security token device peripheral coupled to the security token enabled computer system CS 105 without requiring an actual physical connection. When enabled, the at least one remote device interface application RDI 210 provides security token interface services

for exchanging data with the security token enabled computer system, receiving a user's critical security parameter provided using the user interface UI 85r and routing the user's critical security parameter to the security token ST 75 for user authentication or verification.

[0059] The at least one remote device interface application RDI 210 further provides user prompts and feedback via a display DI 20r.

[0060] The security token ST 75 is operatively coupled to the security token interface device STI 70r by a connection means 60t and includes a public and a private key pair Kpub 225t, Kpri 230 and a reference critical security parameter CSPr 235 retrievably stored in the token memory. At least one token remote access application TRA 215 is likewise installed in the token memory.

[0061] The at least one token remote access application TRA 215 allows the security token ST 75 to establish a secure end-to-end communications connection in conjunction with the security token enabled computer system CS 105, restrict the secure end-to-end communications connection to a single wireless secure communications connection by way of a dedicated wireless communications channel Wc 220w, authenticate a user by comparing a user's provided critical security parameter to the reference critical security parameter CSPr 235 and send an affirmative signal to the security token enabled computer system CS 105 if the user is successfully authenticated. Local communications channel Lc1, Lc2, Lcn 220 allows multiple communications sessions to be established when the ST 75 is locally connected to either the intelligent remote device IRD 110 or security token enabled computer system CS 105.

[0062] The dedicated wireless communications channel Wc 220w restricts the number of communications sessions which can be established remotely. The at least one token remote access application TRA 215 includes an authentication state table 240, 245 which requires fulfillment before access 250t is allowed to one or more secure token resource SRt 255t. In one embodiment of the invention, the communication session is not available to the security token ST 75 until the authentication state table 240, 245 is properly set by authentication of the user.

[0063] The security token enabled computer system 105 includes a wireless transceiver T/R1 compatible with the wireless transceiver T/R2 installed on the intelligent remote device IRD 110 and at least one remote access application RAA 205. The at least one remote access application RAA 205 is generally a middleware application which allows the security token enabled computer system CS 105 to authenticate the security token ST 75, establish the secure end-to-end communications connection with the security token ST 75 over the wireless link 65 and allow the user access 250c to one or more secure resources following a receipt of an affirmative signal sent from the security token ST 75.

[0064] In one embodiment of the invention, the at least one remote access application RAA 205 includes an authentication state table 260, 265 which requires fulfillment before access 250c is allowed to the one or more secure computer system resource SRc 255c. 105. The security token enabled computer system 105 further includes a display 20c which provides a user with information related at least to authentication status 203c.

[0065] The messaging protocol used to communicate with the security token ST 75 includes an ISO 7816 compliant communications protocol. Protocol conversion between higher level packet communications protocols and the lower level ISO 7816 communications protocol may be accomplished by either the remote access application RAA 205 installed on the security token enabled computer system CS 110 or by the remote device interface RDI 210 installed on the intelligent remote device IRD 110.

[0066] A secure arrangement for exchanging APDU commands and responses between the security token ST 75 and security token enabled computer system CS 105 is described in the document US 2002-0162021 A1, to which it can be referred

[0067] Extensible authentication protocols (EAP) as described in the internet standards RFC 2284 or RFC 2716 may be incorporated into the communications connection as well.

[0068] The authentication state tables 240, 245, 260, 265 may be part of a preestablished set of security policies. In one embodiment of the invention, access requirements are determined by the security policies maintained within the security token ST 75 as is described in the document US 2004-0123152 A1, entitled "Uniform Framework for Security Tokens," to which it can be referred.

[0069] Additional security policies may be combined with the security policies established for the security token as is described in the document US 2004-0221174 A 1 and likewise to which it can be referred.

[0070] Referring to Figure 2A, the secure end-to-end communications connection is initiated by a user selecting a remote authentication option 204r from the display DI 20r associated with the intelligent remote device IRD 110. The at least one token remote access application 215 causes the public key Kpub 225t to be sent to the security token enabled computer system CS 105 from the security token ST 75.

[0071] In an alternate embodiment of the invention, no user interaction is required to initiate the secure end-to-end communications connection. In the alternate embodiment of the invention, the communications handshaking between the two wireless transceivers T/R1 60c, T/R2 60r automatically causes execution of the at least one token remote access application 215.

[0072] In the preferred embodiment of the invention, a public key Kpub 225t or duplicate thereof Kpub 225c, is sent to the security token enabled computer system CS 105 in an X.509 certificate where it is retrievably stored. The public key Kpub 225c will be used to authenticate the security token ST 75 to the security token enabled computer system CS 105 and to perform a secure sym-

metric key exchange between the security token enabled computer system CS 105 and security token ST 75.

[0073] Referring to Figure 2B, the receipt of the public key Kpub 225c causes the at least one remote access application to generate a challenge [C] 270c which is then encrypted 275e using the public key Kpub 225c and the resulting cryptogram [C]Kpub 280c is then sent over the wireless link 65 to the security token ST 75.

[0074] The display DI 20c associated with the security token enabled computer system CS 105 provides user feedback 205c that a remote authentication transaction has been initiated. The at least one token remote access application TRA 215 receives and decrypts 275d the cryptogram [C]Kpub 280c using the counterpart private key Kpri 230 generating the token clear text response [C] 270r to the challenge.

[0075] Referring to Figure 2C, the token response to the challenge [C] 270r is returned to the security token enabled computer system CS 105 where the remote access application RAA 205 compares 222 the returned response [C] 270r to the initial challenge [C] 270c. If the token response [C] 270r matches the initial challenge [C] 270c, the PKI authentication part of the computer systems authentication state table is fulfilled 260. If the security token ST 75 fails this first authentication transaction processing ends and a new attempt to establish the secure end-to-end communications connection will need to be performed.

[0076] Referring to Figure 2D, a first part of the anonymous secure end-to-end communications connection is initiated by the remote access application RAA 205 generating a symmetric key set. The symmetric key sets KSt 285t and KSc 285s are identical symmetric keys generated or derived from a random number preferably having sufficient bit strength of at least 64 bits to assure adequate security and performance.

[0077] The at least one remote access application RAA 205 encrypts 275e one of the symmetric keys KSt 285t using the public key Kpub 225c and the resulting cryptogram [KSt]Kpub 290t is then sent over the wireless link 65 to the security token ST 75. In one embodiment of the invention, a channel identifier Wc 220w is included in a message header associated with the cryptogram which specifies the dedicated communications channel in which the symmetric key is to be used. The at least one token remote access application TRA 215 receives and decrypts 275d the cryptogram [KSt]Kpub 290t using the counterpart private key Kpri 230 restoring the token's shared symmetric key KSt 285t.

[0078] Referring to Figure 2E, the token shared symmetric key KSt 285t is assigned to the dedicated communications channel Wc 220w which establishes the secure end-to-end communications connection 200. The share symmetric keys KSt 285t, KSc 285c are used as block cipher keys during information exchange over the secure end-to-end communications connection. The establishment of the secure end-to-end communications connection 200 fulfills a first element of the token's authentication state table 240. The dedicated communications channel restricts the secure end-to-end communications connection to a single wireless secure communications connection 200 with the security token to prevent unauthorized entities from eavesdropping on subsequent security token transactions.

[0079] Referring to Figure 2F, the final security transaction is performed where the user is prompted 206r on the display 20r associated with the intelligent remote device IRD 110 to provide his or her critical security parameter CSPu 235u. The user's critical security parameter CSPu 235u is inputted 295 to the intelligent remote device IRD 110 via the user interface UI 85 and routed to the security token ST 75 for authentication.

[0080] The user's critical security parameter CSPu 235 is compared 227 to the reference critical security parameter CSPr 235r by the token remote access application TRA 215. If a match is found between the user's critical security parameter CSPu 235 and the reference critical security parameter CSPr 235r, the critical security parameter CSP 245 element of the token's authentication state table is fulfilled. If the critical security parameter fails this second authentication transaction processing ends and a new attempt to establish the secure end-to-end communications connection will need to be performed.

[0081] Referring to Figure 2G, the final phase of the invention implementation is depicted where an affirmative result signal 299t is transmitted from the security token ST 75 to the security token enabled computer system via the secure end-to-end communications connection 200. The receipt of the affirmative result signal 299c fulfills the second element ST 265 of the computer system's authentication state table which allows access 250t, 250c to the one or more secure resources 255t, 255c associated with the security token ST 75, security token enabled computer system CS 105 or both devices.

[0082] The user display DI 20r associated with intelligent remote device IRD 110 optionally provides at least visual indication 208r that a secure messaging session is in progress. Likewise, the user display DI 20c associated with the security token enabled computer system CS 105 provides at least visual indication 207c that access has been granted remotely. Other types of visual, aural and vibratory feedback are envisioned as well.

[0083] Referring to Figure 3, the major steps for implementing the invention are depicted. The process is initiated 300 by establishment of a wireless communications connection between a security token enabled computer system and an intelligent remote device having a security token operatively coupled thereto. A public key is sent from the security token via the intelligent remote device to the security token enabled computer system 310, preferably as part of an X.509 formatted digital certificate. Transfer of the public key may be automatically performed during a communications handshake or by user interaction.

[0084] The security token enabled computer system

authenticates 315 the security token using a challenge/response protocol, whereby a challenge is generated, encrypted using the received public key, then transmitted to the security token over the wireless communications connection. The security token receives the cryptogram and decrypts the challenge using a private key counterpart of the public key. The clear text challenge is then returned to the security token enabled computer system for authentication. If the security token is not authenticated 320 processing ends 370. If the security token is authenticated 320, a symmetric key set is generated on the security token enabled computer system 325 and a secure key exchange 330 performed with the security token, whereby at least one of the symmetric keys is encrypted using the public key and sent over the wireless communications connection to the security token.

[0085] The received encrypted symmetric key is decrypted using the private key, assigned to a dedicated communications channel and the dedicated communications channel locked if a predetermined limit of preexisting wireless communications connections is not exceeded 335. If the predetermined limit is exceeded 345, processing ends 375. The predetermined limit is usually set to 1 in the preferred embodiment of the invention.

[0086] A first security state is set by either or both the security token and/or security token enabled computer system which indicates that a secure communications channel has been established. In one embodiment of the invention, the secure communications channel is not enabled until the user is authenticated as described below.

[0087] If the predetermined limit is not exceeded 345, the user is prompted 350 to provide his or her critical security parameter to the intelligent remote device. The provided critical security parameter is then authenticated 355 by the security token by comparing a reference critical security parameter to the received critical security parameter. If the user is not authenticated 360, processing ends. If the user is authenticated 355, an affirmative result signal is generated by the security token and sent to the security token enabled computer system 365. Receipt of the affirmative result signal allows access to one or more secure resources 370. Processing ends 375 normally at the conclusion of the secure communications session by the user, removal of the security token from the intelligent remote device or moving outside of a predetermined proximity range from the security token enabled computer system.

[0088] The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. No specific limitation is intended to a particular security token operating environment. Other variations and embodiments are possible in light of above teachings, and it is not intended that this Detailed Description limit the scope of invention, but rather by the Claims that follow herein.

Claims

1. A method for establishing a secure end-to-end communications connection between a security token enabled computer system (105) and a security token (75) associated with a wireless intelligent remote device (110) comprising the steps of:

   a. performing a first security transaction which authenticates said security token (75) to said security token enabled computer system (105),
   b. establishing a secure communications connection between said security token (75) and said security token enabled computer system (105) which incorporates a shared symmetric key set (285t, 285s) generated during said first security transaction,
   c. assigning at least one key (285t) from said shared symmetric key set (285t, 285s) to a dedicated communications channel (220w) between the security token enabled computer system (105) and the security token (75), accessible to said security token (751) and
   d. setting at least a first security state indicating that the secure dedicated communications channel (220) has been established,
   e. performing a second security transaction, following said first security transaction, which authenticates a user to said security token (75) by providing a critical security parameter (235) to said security token via said intelligent remote device (110),
   f. transmitting an affirmative result signal from the security token (75) to the security token enabled computer system (105) via the secure end-to-end communications connection if the user is authenticated and setting at least a second security state indicating that the user is authenticated by the security token (75), and
   g. enabling the use of said secure communications connection following the setting of said at least a second security state.

2. The method according to claim 1 wherein said secure communications connection is anonymous to but controlled by said security token (75).

3. The method according to claim 1 wherein said first security transaction comprises a challenge/response protocol which incorporates an asymmetric key pair.

4. The method according to claim 1 further including the step of signaling said security token enabled

computer system (105) by said security token (75) if said second security transaction is successful.

5. The method according to claim 1 wherein said secure communications connection is established at least in part over a wireless telecommunications connection.

6. The method according to claim 1 further including the step of allowing said user access to one or more secure resources following successful completion of said second security transaction.

7. The method according to claim 1 wherein step 1.b further includes the steps of:

1 b.1 generating said shared symmetric key set (285t, 285s) by said security token enabled computer system (105).
1 b.2 encrypting said at least one key (285t) with a public key (225c) associated with said security token (75).
1 b.3 sending the encrypted said at least one key (285t) to said security token (75), and
1 b.4 decrypting the said at least one key (285t) with a private key (230) associated with said security token (75).

8. The method according to claim 1 wherein said dedicated communications channel (220w) prevents the number of concurrent wireless secure communications connections with said security token (75) from exceeding a predetermined limit.

9. The method according to claim 8 wherein said predetermined limit is 1.

10. The method according to claim 6 wherein said secure communications connection is only available when said security token (75) is inside of a predefined range from the said security token enabled computer system (105).

11. A method recording to claim 1, further comprising the step of establishing a wireless communications connection between said intelligent remote device (110) and said security token enabled computer system (105).

12. The method according to claim 11 further including the step of allowing said user access to one or more secure resources (255t, 255c) following successful completion of said second security transaction.

13. The method according to claim 11 wherein step e further includes the steps of e 1 prompting said user to provide said critical security parameter (235).

14. The method according to claim 11 further including the step of sending a digital certificate to said security token enabled computer system (105).

15. The method according to claim 11 further including the step of prompting said user to select either a local or remote authentication transaction.

16. The method according to claim 11 further including the step of providing said user a sensory feedback (205c) from at least said security token enabled computer system (105) indicative of a remote authentication transaction in progress.

17. The method according to claim 11 wherein said wireless secure communications connection is associated with a dedicated communications channel (220w) which prevents concurrent wireless secure communications connections from being established with said security token (75).

18. The method according to claim 16 wherein said sensory feedback (205c) includes visual, tactile, aural or vibratory feedback.

19. The method according to claim 11 wherein said wireless secure communications connection is only available when said security token (75) is inside a predefined range from the said security token enabled computer system (105).

20. A system for establishing a secure end-to-end communications connection between a security token enabled computer system (105) and a security token (75) associated with a wireless intelligent remote device (110) comprising;

said security token enabled computer system (105) including:

a first security transaction, means for at least authenticating said security token (75) to said security token enabled computer system (105):
a first secure communications connection means for at least establishing a secure communications connection between said security token enabled computer system (105) and said security token (75);

wherein

said intelligent remote device (110) includes;
a security token interface (70r) means for at least operatively coupling said security token (75) to said intelligent remote device (110):

a user interface (85r) means for at least receiving and routing a critical security parameter (235) provided by said user to said security token interface (70r) means:

said security token (75) incudes:

a second secure communications connection means for at least establishing said secure communications connection in conjunction with said first secure communications connection means;
a dedicated communications channel (220w) means for preventing a concurrent secure communications connection from being established with said security token (75); and

a second security transaction means for at least authenticating said user to said security token (75), after said first security transaction, using at least said critical security parameter (235);
in that the system comprises means for activating said user interface means (85r) for receiving and routing said critical security parameter (235), once said first secure communications connection means have established said secure communications connection;
and in that the system comprises means for transmitting an affirmative result signal from the security token (75) to the security token enabled compute system (105) via the secure end-to-end communications connection if the user is authenticated.

21. The system according to claim 20 wherein said security token enabled computer system (105) is in wireless communications with said intelligent remote device (110) and said operatively coupled security token (75).

22. The system according to claim 20 wherein said first security transaction means includes a challenge/response protocol means and an asymmetric cryptography means.

23. The system according to claim 20 wherein said first secure communications connection means includes a symmetric key set generation means and a secure symmetric key exchange means.

24. The system according to claim 20 wherein said security token interface (70r) means includes security token communications means and electromagnetic power transfer means.

25. The system according to claim 20 wherein said dedicated communications channel means (220w) includes a unique channel identifier means which is accessible by said security token enabled computer system (105).

26. The system according to claim 20 wherein successful execution of said first security transaction means sets a first computer system security state associated with said security token (75) enabled client.

27. The system according to claim 20 wherein establishment of said secure communications connection sets a first token security state associated with said security token (75).

28. The system according to claim 20 wherein successful execution of said second security transaction means sets a second token (75) security state associated with said security token (75).

29. The system according to claim 20 wherein said security token enabled computer system (105) further includes proximity sensing means (115c).

30. A system according to claim 20 wherein:

said security token enabled computer system (105) includes;

a first processor (5c):
a first memory (10c) coupled to said first processor (5c);
at least one remote authentication application operatively stored in a first portion of said first memory having logical instructions executable by said first processor (5c) to;
perform said authenticating said security token (75);
establish said secure communications connection with said security token (75);

said intelligent remote device (110) includes:

a second processor (5r):
a second memory (10r) coupled to said second processor (5r);
a security token interface (70r) coupled to said second processor (5r);
a user interface (85r) coupled to said second processor (5r); and,
at least one remote device interface application operatively stored in a portion of said second memory (10r) having logical instructions executable by said second processor (5r) to;
emulate a security token device interface locally coupled to at least said security token enabled computer system (105); and,
conditionally receive and route said critical

security parameter (235) provided by said user via said user interface (85r) to said security token (75); and

said security token (75) includes;

at least a third processor (5t);
a third memory coupled to said at least a third processor (5t);
a communications and electromagnetic power interface coupled to said at least a third processor (5t) and said security token interface (70r):
at least one token remote authentication application operatively stored in a second portion of said third memory having logical instructions executable by said at least a third processor (5t) to:

establish said secure communications connection with said security token enabled computer system (105);
restrict said secure communications connection to a single wireless communications channel; and
perform said authenticating said user based at least in part on said critical security parameter (235).

31. The system according to claim 30 further including a first wireless transceiver (60c) functionally coupled to said first processor (5c) in processing communications with a second wireless transceiver (60r) functionally coupled to said second processor (5r).

32. The system according to claim 30 further including a public key (225c) associated with said security token (75) retrievably stored in a second portion of said first memory (10c) and a private key (230) retrievably stored in a second portion of said third memory, wherein said private key (230) is a counterpart to said public key (225c).

33. The system according to claim 30 further including a reference critical security parameter (235r) retrievably stored in a third portion of said third memory.

34. The system according to claim 32 wherein said public (225c) and private (230) keys are incorporated into said challenge/response protocol used to authenticate said security token (75) to said security token enabled computer system (105).

35. The system according to claim 34 wherein said at least one remote authentication application further includes logical instructions executable by said first processor (5c) to generate said symmetric key set (285t, 285s) and perform a secure key exchange with said security token (75).

36. The system according to claim 35 wherein said secure key exchange is performed using said public (225c) and private (230) keys.

37. The system according to claim 35 wherein said symmetric key set (285t, 285s) is incorporated into said secure end-to-end communications connection.

38. The system according to claim 30 wherein said user is authenticated by said at least one token remote authentication application by comparing said provided critical security parameter (235) to said reference critical security parameter (235r).

39. The system according to claim 30 wherein said at least one token remote authentication application restricts usage of said secure end-to-end communications connection until said user is authenticated.

40. The system according to claim 30 wherein said secure end-to-end communications connection is restricted to a single wireless connection with said security token (75) using a dedicated communications channel (220w) controlled by said at least one token remote authentication application.

41. The system according to claim 36 wherein said dedicated communications channel (220w) includes a unique identifier available by said security token enabled computer system (105).

42. The system according to claim 30 wherein said communications and electromagnetic power interface includes inductive means, capacitive means or electric contact means.

43. A computer program product embodied in a tangible form readable by a security token processor (5t), wherein said computer program product includes executable instructions stored thereon for implementing the method of claim 1.

44. The computer program product according to claim 43 wherein said tangible form includes magnetic media, optical media or logical media.

45. The computer program product according to claim 43 wherein said executable instructions are stored in a code format comprising byte code, compiled, interpreted, compliable and interpretable.

Patentansprüche

1. Verfahren zum Einrichten einer sicheren Ende-Ende-Kommunikationsverbindung zwischen einem Si-

cherheits-Token-aktivierten Computersystem (105) und einem Sicherheits-Token (75), das einer drahtlosen intelligenten fernen Vorrichtung (110) zugeordnet ist, welches folgende Schritte aufweist:

a. Ausführen einer ersten Sicherheitstransaktion, welche das Sicherheits-Token (75) für das Sicherheits-Token-aktivierte Computersystem (105) authentifiziert,
b. Einrichten einer sicheren Kommunikationsverbindung zwischen dem Sicherheits-Token (75) und dem Sicher-heits-Token-aktivierten Computersystem (105), welches einen während der ersten Sicherheitstransaktion erzeugten geteilten symmetrischen Schlüsselsatz (285t, 285s) aufweist,
c. Zuweisen mindestens eines Schlüssels (285t) von dem geteilten symmetrischen Schlüsselsatz (285t, 285s) zu einem zweckgebundenen Kommunikationskanal (220w) zwischen dem Sicherheits-Token-aktivierten Computersystem (105) und dem Sicherheits-Token (75), welcher dem Sicherheits-Token (751) zugänglich ist, und
d. Festlegen mindestens eines ersten Sicherheitszustands, welcher angibt, dass der sichere zweckgebundene Kommunikationskanal (220) eingerichtet worden ist,
e. Ausführen einer zweiten Sicherheitstransaktion nach der ersten Sicherheitstransaktion, welche einen Benutzer für das Sicherheits-Token (75) authentifiziert, indem ein kritischer Sicherheitsparameter (235) dem Sicherheits-Token über die intelligente ferne Vorrichtung (110) bereitgestellt wird,
f. Senden eines bestätigenden Ergebnissignals von dem Sicherheits-Token (75) zu dem Sicherheits-Token-aktivierten Computersystem (105) über die sichere Ende-Ende-Kommunikationsverbindung, falls der Benutzer authentifiziert ist, und Festlegen mindestens eines zweiten Sicherheitszustands, welcher angibt, dass der Benutzer durch das Sicherheits-Token (75) authentifiziert ist, und
g. Aktivieren der Verwendung der sicheren Kommunikationsverbindung nach dem Festlegen des mindestens einen zweiten Sicherheitszustands.

2. Verfahren nach Anspruch 1, wobei die sichere Kommunikationsverbindung für das Sicherheits-Token (75) anonym ist, jedoch von diesem gesteuert wird.

3. Verfahren nach Anspruch 1, wobei die erste Sicherheitstransaktion ein Herausforderung/Antwort-Protokoll [Challenge/Response Protocol] aufweist, welches ein asymmetrisches Schlüsselpaar aufweist.

4. Verfahren nach Anspruch 1, bei dem ferner dem Sicherheits-Token-aktivierten Computersystem (105) durch das Sicherheits-Token (75) signalisiert wird, ob die zweite Sicherheitstransaktion erfolgreich ist.

5. Verfahren nach Anspruch 1, wobei die sichere Kommunikationsverbindung zumindest teilweise über eine drahtlose Telekommunikationsverbindung eingerichtet wird.

6. Verfahren nach Anspruch 1, bei dem ferner dem Benutzer Zugang zu einer oder mehreren sicheren Ressourcen gewährt wird, nachdem die zweite Sicherheitstransaktion erfolgreich abgeschlossen worden ist.

7. Verfahren nach Anspruch 1, wobei Schritt 1.b ferner folgende Schritte aufweist:

1 b.1 Erzeugen des geteilten symmetrischen Schlüsselsatzes (285t, 285s) durch das Sicherheits-Token-aktivierte Computersystem (105),
1 b.2 Verschlüsseln des mindestens einen Schlüssels (285t) mit einem öffentlichen Schlüssel (225c), der dem Sicherheits-Token (75) zugeordnet ist,
1 b.3 Senden des mindestens einen verschlüsselten Schlüssels (285t) zu dem Sicherheits-Token (75) und
1 b.4 Entschlüsseln des mindestens einen Schlüssels (285t) mit einem privaten Schlüssel (230), der dem Sicherheits-Token (75) zugeordnet ist.

8. Verfahren nach Anspruch 1, wobei der zweckgebundene Kommunikationskanal (220w) verhindert, dass die Anzahl der gleichzeitigen drahtlosen sicheren Kommunikationsverbindungen mit dem Sicherheits-Token (75) eine vorgegebene Grenze überschreitet.

9. Verfahren nach Anspruch 8, wobei die vorgegebene Grenze 1 ist.

10. Verfahren nach Anspruch 6, wobei die sichere Kommunikationsverbindung nur verfügbar ist, wenn sich das Sicherheits-Token (75) innerhalb eines vordefinierten Bereichs von dem Sicherheits-Token-aktivierten Computersystem (105) befindet.

11. Verfahren nach Anspruch 1, bei dem ferner eine drahtlose Kommunikationsverbindung zwischen der intelligenten fernen Vorrichtung (110) und dem Sicherheits-Token-aktivierten Computersystem (105) eingerichtet wird.

12. Verfahren nach Anspruch 11, bei dem ferner dem Benutzer Zugang zu einer oder mehreren sicheren Ressourcen (255t, 255c) gewährt wird, nachdem die

zweite Sicherheitstransaktion erfolgreich abgeschlossen worden ist.

13. Verfahren nach Anspruch 11, wobei in Schritt e ferner der Benutzer in Schritt e 1 aufgefordert wird, den kritischen Sicherheitsparameter (235) bereitzustellen.

14. Verfahren nach Anspruch 11, bei dem ferner ein digitales Zertifikat zu dem Sicherheits-Token-aktivierten Computersystem (105) gesendet wird.

15. Verfahren nach Anspruch 11, bei dem ferner der Benutzer aufgefordert wird, entweder eine lokale oder eine ferne Authentifizierungstransaktion auszuwählen.

16. Verfahren nach Anspruch 11, bei dem ferner dem Benutzer eine sensorische Rückmeldung (205c) zumindest von dem Sicherheits-Token-aktivierten Computersystem (105) bereitgestellt wird, welche angibt, dass eine ferne Authentifizierungstransaktion abläuft.

17. Verfahren nach Anspruch 11, wobei die drahtlose sichere Kommunikationsverbindung einem zweckgebundenen Kommunikationskanal (220w) zugeordnet ist, der verhindert, dass gleichzeitige drahtlose sichere Kommunikationsverbindungen mit dem Sicherheits-Token (75) eingerichtet werden.

18. Verfahren nach Anspruch 16, wobei die sensorische Rückmeldung (205c) eine sichtbare, fühlbare, hörbare oder vibratorische Rückmeldung einschließt.

19. Verfahren nach Anspruch 11, wobei die drahtlose sichere Kommunikationsverbindung nur verfügbar ist, wenn sich das Sicherheits-Token (75) innerhalb eines vordefinierten Bereichs von dem Sicherheits-Token-aktivierten Computersystem (105) befindet.

20. System zum Einrichten einer sicheren Ende-Ende-Kommunikationsverbindung zwischen einem Sicherheits-Token-aktivierten Computersystem (105) und einem Sicherheits-Token (75), das einer drahtlosen intelligenten fernen Vorrichtung (110) zugeordnet ist, welches aufweist:

das Sicherheits-Token-aktivierte Computersystem (105), welches umfasst:

eine erste Sicherheitstransaktionseinrichtung zumindest zum Authentifizieren des Sicherheits-Tokens (75) für das Sicherheits-Token-aktivierte Computersystem (105),
eine erste sichere Kommunikationsverbindungseinrichtung zumindest zum Einrichten einer sicheren Kommunikationsverbindung zwischen dem Sicherheits-Token-aktivierten Computersystem (105) und dem Sicherheits-Token (75), wobei die intelligente ferne Vorrichtung (110) aufweist:
eine Sicherheits-Token-Schnittstelleneinrichtung (70r) zumindest zum operativen Koppeln des Sicherheits-Tokens (75) mit der intelligenten fernen Vorrichtung (110),
eine Benutzerschnittstelleneinrichtung (85r) zumindest zum Empfangen und Weiterleiten eines kritischen Sicherheitsparameters (235), der der Sicherheits-Token-Schnittstelleneinrichtung (70r) von dem Benutzer bereitgestellt wird,

das Sicherheits-Token (75) aufweist:

eine zweite sichere Kommunikationsverbindungseinrichtung zumindest zum Einrichten der sicheren Kommunikationsverbindung in Zusammenhang mit der ersten sicheren Kommunikationsverbindungseinrichtung,
eine zweckgebundene Kommunikationskanaleinrichtung (220w) zum Verhindern, dass eine gleichzeitige sichere Kommunikationsverbindung mit dem Sicherheits-Token (75) eingerichtet wird, und

eine zweite Sicherheitstransaktionseinrichtung zumindest zum Authentifizieren des Benutzers für das Sicherheits-Token (75) nach der ersten Sicherheitstransaktion unter Verwendung zumindest des kritischen Sicherheitsparameters (235),
das System eine Einrichtung zum Aktivieren der Benutzerschnittstelleneinrichtung (85r) zum Empfangen und Weiterleiten des kritischen Sicherheitsparameters (235), sobald die erste sichere Kommunikationsverbindungseinrichtung die sichere Kommunikationsverbindung eingerichtet hat, aufweist,
und das System eine Einrichtung zum Senden eines bestätigenden Ergebnissignals von dem Sicherheits-Token (75) zu dem Sicherheits-Token-aktivierten Computersystem (105) über die sichere Ende-Ende-Kommunikationsverbindung, falls der Benutzer authentifiziert ist, aufweist.

21. System nach Anspruch 20, wobei das Sicherheits-Token-aktivierte Computersystem (105) in Drahtloskommunikation mit der intelligenten fernen Vorrichtung (110) und dem operativ gekoppelten Sicherheits-Token (75) steht.

22. System nach Anspruch 20, wobei die erste Sicher-

heitstransaktionseinrichtung eine Herausforderung/Antwort-Protokolleinrichtung [Challenge/Response Protocol Means] und eine asymmetrische Kryptographieeinrichtung aufweist.

23. System nach Anspruch 20, wobei die erste sichere Kommunikationsverbindungseinrichtung eine Einrichtung zum Erzeugen eines symmetrischen Schlüsselsatzes und eine Einrichtung zum Austauschen sicherer symmetrischer Schlüssel aufweist.

24. System nach Anspruch 20, wobei die Sicherheits-Token-Schnittstelleneinrichtung (70r) eine Sicherheits-Token-Kommunikationseinrichtung und eine Einrichtung zum Übertragen elektromagnetischer Energie aufweist.

25. System nach Anspruch 20, wobei die zweckgebundene Kommunikationskanaleinrichtung (220w) eine eindeutige Kanalidentifiziereinrichtung aufweist, die für das Sicherheits-Token-aktivierte Computersystem (105) zugänglich ist.

26. System nach Anspruch 20, wobei die erfolgreiche Ausführung der ersten Sicherheitstransaktionseinrichtung einen dem Sicherheits-Token-(75)-aktivierten Client zugeordneten ersten Computersystem-Sicherheitszustand festlegt.

27. System nach Anspruch 20, wobei das Einrichten der sicheren Kommunikationsverbindung einen dem Sicherheits-Token (75) zugeordneten ersten Token-Sicherheitszustand festlegt.

28. System nach Anspruch 20, wobei die erfolgreiche Ausführung der zweiten Sicherheitstransaktionseinrichtung einen dem Sicherheits-Token (75) zugeordneten zweiten Token-Sicherheitszustand festlegt.

29. System nach Anspruch 20, wobei das Sicherheits-Token-aktivierte Computersystem (105) ferner eine Näherungserfassungseinrichtung (115c) aufweist.

30. System nach Anspruch 20, wobei:

das Sicherheits-Token-aktivierte Computersystem (105) aufweist:

einen ersten Prozessor (5c),
einen ersten Speicher (10c), der mit dem ersten Prozessor (5c) gekoppelt ist,
mindestens eine ferne Authentifizierungsanwendung, die operativ in einem ersten Abschnitt des ersten Speichers gespeichert ist, der logische Anweisungen aufweist, die von dem ersten Prozessor (5c) ausführbar sind, um folgendes vorzunehmen:

Ausführen der Authentifizierung des Sicherheits-Tokens (75) und
Einrichten der sicheren Kommunikationsverbindung mit dem Sicherheits-Token (75),

wobei die intelligente ferne Vorrichtung (110) aufweist:

einen zweiten Prozessor (5r),
einen zweiten Speicher (10r), der mit dem zweiten Prozessor (5r) gekoppelt ist,
eine Sicherheits-Token-Schnittstelle (70r), die mit dem zweiten Prozessor (5r) gekoppelt ist,
eine Benutzerschnittstelle (85r), die mit dem zweiten Prozessor (5r) gekoppelt ist, und
mindestens eine ferne Vorrichtungsschnittstellenanwendung, die operativ in einem Abschnitt des zweiten Speichers (10r) gespeichert ist, der logische Anweisungen aufweist, die von dem zweiten Prozessor (5r) ausführbar sind, um folgendes vorzunehmen:

Emulieren einer Sicherheits-Token-Vorrichtungs-schnittstelle, die lokal zumindest mit dem Sicherheits-Token-aktivierten Computersystem (105) gekoppelt ist, und
bedingtes Empfangen und Weiterleiten des kritischen Sicherheitsparameters (235), der dem Sicherheits-Token (75) vom Benutzer über die Benutzerschnittstelle (85r) bereitgestellt wird, und

das Sicherheits-Token (75) aufweist:

mindestens einen dritten Prozessor (5t),
einen dritten Speicher, der mit dem mindestens einen dritten Prozessor (5t) gekoppelt ist,
eine Schnittstelle für Kommunikation und elektromagnetische Energie, die mit dem mindestens einen dritten Prozessor (5t) und der Sicherheits-Token-Schnittstelle (70r) gekoppelt ist,
mindestens eine ferne Token-Authentifizierungsanwendung, die in einem zweiten Abschnitt des dritten Speichers operativ gespeichert ist, der logische Anweisungen aufweist, die von dem mindestens einen dritten Prozessor (5t) ausführbar sind, um folgendes auszuführen:

Einrichten der sicheren Kommunikati-

onsverbindung mit dem Sicherheits-Token-aktivierten Computersystem (105),
Beschränken der sicheren Kommunikationsverbindung auf einen einzigen drahtlosen Kommunikationskanal und
Ausführen der Authentifizierung des Benutzers auf der Grundlage zumindest teilweise des kritischen Sicherheitsparameters (235).

31. System nach Anspruch 30, welches ferner einen ersten Drahtlos-Transceiver (60c) aufweist, der bei der Verarbeitung von Kommunikationen mit einem zweiten Drahtlos-Transceiver (60r), der funktionell mit dem zweiten Prozessor (5r) gekoppelt ist, funktionell mit dem ersten Prozessor (5c) gekoppelt ist.

32. System nach Anspruch 30, welches ferner einen dem Sicherheits-Token (75) zugeordneten öffentlichen Schlüssel (225c), der abrufbar in einem zweiten Abschnitt des ersten Speichers (10c) gespeichert ist, und einen privaten Schlüssel (230), der abrufbar in einem zweiten Abschnitt des dritten Speichers gespeichert ist, aufweist, wobei der private Schlüssel (230) ein Gegenstück des öffentlichen Schlüssels (225c) ist.

33. System nach Anspruch 30, welches ferner einen kritischen Referenz-sicherheitsparameter (235r) aufweist, der abrufbar in einem dritten Abschnitt des dritten Speichers gespeichert ist.

34. System nach Anspruch 32, wobei der öffentliche Schlüssel (225c) und der private Schlüssel (230) in das Herausforderung/Antwort-Protokoll aufgenommen sind, das verwendet wird, um das Sicherheits-Token (75) für das Sicherheits-Token-aktivierte Computersystem (105) zu authentifizieren.

35. System nach Anspruch 34, wobei die mindestens eine ferne Authentifizierungsanwendung ferner logische Anweisungen aufweist, die von dem ersten Prozessor (5c) ausführbar sind, um den symmetrischen Schlüsselsatz (285t, 285s) zu erzeugen und einen sicheren Schlüsselaustausch mit dem Sicherheits-Token (75) auszuführen.

36. System nach Anspruch 35, wobei der sichere Schlüsselaustausch unter Verwendung des öffentlichen Schlüssels (225c) und des privaten Schlüssels (230) ausgeführt wird.

37. System nach Anspruch 35, wobei der symmetrische Schlüsselsatz (285t, 285s) in die sichere Ende-Ende-Kommunikationsverbindung aufgenommen ist.

38. System nach Anspruch 30, wobei der Benutzer durch die mindestens eine ferne Token-Authentifizierungsanwendung authentifiziert wird, indem der bereitgestellte kritische Sicherheitsparameter (235) mit dem kritischen Referenz-sicherheitsparameter (235r) verglichen wird.

39. System nach Anspruch 30, wobei die mindestens eine ferne Token-Authentifizierungsanwendung die Verwendung der sicheren Ende-Ende-Kommunikationsverbindung beschränkt, bis der Benutzer authentifiziert worden ist.

40. System nach Anspruch 30, wobei die sichere Ende-Ende-Kommunikationsverbindung unter Verwendung eines zweckgebundenen Kommunikationskanals (220w), der durch die mindestens eine ferne Token-Authentifizierungsanwendung gesteuert wird, auf eine einzige drahtlose Verbindung mit dem Sicherheits-Token (75) beschränkt wird.

41. System nach Anspruch 36, wobei der zweckgebundene Kommunikationskanal (220w) eine eindeutige Kennung aufweist, die dem Sicherheits-Token-aktivierten Computersystem (105) zur Verfügung steht.

42. System nach Anspruch 30, wobei die Schnittstelle für Kommunikation und elektromagnetische Energie induktive Einrichtungen, kapazitive Einrichtungen oder elektrische Kontakteinrichtungen aufweist.

43. Computerprogrammprodukt, das in einer durch einen Sicherheits-Token-Prozessor (5t) lesbaren konkreten Form verwirklicht ist, wobei das Computerprogrammprodukt darauf gespeicherte ausführbare Anweisungen aufweist, um das Verfahren nach Anspruch 1 zu implementieren.

44. Computerprogrammprodukt nach Anspruch 43, wobei die konkrete Form magnetische Medien, optische Medien oder logische Medien aufweist.

45. Computerprogrammprodukt nach Anspruch 43, wobei die ausführbaren Anweisungen in einem Codeformat gespeichert sind, das Bytecode, ein kompiliertes Codeformat, ein interpretiertes Codeformat und ein kompilierbares und interpretierbares Codeformat einschließt.

Revendications

1. Procédé pour établir une connexion de communications sécurisée de bout en bout entre un système d'ordinateur activé par jeton de sécurité (105) et un jeton de sécurité (75) associé à un dispositif intelligent sans fil situé à distance (110) comprenant les étapes consistant à :

a. effectuer une première transaction sécurisée qui authentifie le jeton de sécurité (75) au système d'ordinateur activé par jeton de sécurité (105),
b. établir une liaison de communications sécurisées entre le jeton de sécurité (75) et le système d'ordinateur activé par jeton de sécurité (105) qui incorpore un jeu de clés symétriques partagées (285t, 285s) produit pendant la première transaction de sécurité,
c. assigner au moins une clé (285t) à partir du jeu de clés symétriques partagées (285t, 285s) à un canal de communication dédié (220w) entre le système d'ordinateur activé par jeton de sécurité (105) et le jeton de sécurité (75), accessible au jeton de sécurité (751) et
d. fixer au moins un premier état de sécurité indiquant que le canal de communication sécurisé dédié (220) a été établi,
e. effectuer une seconde transaction de sécurité, après la première transaction de sécurité, qui authentifie un utilisateur au jeton de sécurité (75) en fournissant un paramètre de sécurité critique (235) au jeton de sécurité par l'intermédiaire du dispositif intelligent sans fil situé à distance (110)
f. transmettre un signal de résultat affirmatif en provenance du jeton de sécurité (75) au système d'ordinateur activé par jeton de sécurité (105) par l'intermédiaire d'une connexion de communications sécurisées de bout en bout si l'utilisateur est authentifié et fixer au moins un second état de sécurité indiquant que l'utilisateur est authentifié par le jeton de sécurité (75), et
g. activer l'utilisation de la connexion de communications sécurisées après la fixation dudit au moins un second état de sécurité

2. Procédé selon la revendication 1, **caractérisé en ce que** la connexion de communications sécurisées est anonyme pour le jeton de sécurité (75) mais commandée par celui-ci.

3. Procédé selon la revendication 1, **caractérisé en ce que** la première transaction de sécurité comprend un protocole challenge/réponse qui incorpore une paire de clés asymétriques.

4. Procédé selon la revendication 1, **caractérisé en ce qu'**il comprend de plus l'étape consistant à signaler au système d'ordinateur activé par jeton de sécurité (105) par le jeton de sécurité (75) si la seconde transaction de sécurité a réussi.

5. Procédé selon la revendication 1, **caractérisé en ce que** la connexion de communications sécurisées est établie au moins en partie au moyen d'une connexion de télécommunications sans fil.

6. Procédé selon la revendication 1, **caractérisé en ce qu'**il comprend de plus l'étape consistant à permettre un accès utilisateur à une ou plusieurs ressources sécurisées après réalisation avec succès de la seconde transaction de sécurité.

7. Procédé selon la revendication 1, **caractérisé en ce que** l'étape 1.b comprend de plus les étapes consistant à :

1b.1 produire le jeu de clés symétriques partagées (285t, 285s) par le système d'ordinateur activé par jeton de sécurité (105).
1b.2 crypter ladite au moins une clé (285t) avec une clé publique (225c) associée au jeton de sécurité (75).
1b.3 envoyer ladite au moins une clé cryptée (285t) au jeton de sécurité (75), et
1b.4 décrypter ladite au moins une clé (285t) avec une clé privée (230) associée au jeton de sécurité (75).

8. Procédé selon la revendication 1, **caractérisé en ce que** le canal de communications dédié (220w) empêche le nombre de connexions de communications sécurisées sans fil concourantes avec le jeton de sécurité (75) de dépasser une limite prédéterminée.

9. Procédé selon la revendication 8 **caractérisé en ce que** la limite prédéterminée est 1.

10. Procédé selon la revendication 6, **caractérisé en ce que** la connexion de communications sécurisées est uniquement disponible lorsque le jeton de sécurité (75) est à l'intérieur d'une plage prédéfinie provenant du système d'ordinateur activé par jeton de sécurité (105).

11. Procédé selon la revendication 1, **caractérisé en ce qu'**il comprend de plus l'étape consistant à établir une connexion de communications sans fil entre le dispositif intelligent sans fil situé à distance (110) et le système d'ordinateur activé par jeton de sécurité (105).

12. Procédé selon la revendication 11, **caractérisé en ce qu'**il comprend de plus l'étape consistant à permettre un accès utilisateur à une ou plusieurs ressources sécurisées (255t, 255e) après réalisation avec succès de la seconde transaction de sécurité.

13. Procédé selon la revendication 11, **caractérisé en ce que** l'étape e comprend de plus l'étape e1 consistant à inviter l'utilisateur à fournir le paramètre de sécurité critique (235).

14. Procédé selon la revendication 11, **caractérisé en ce qu'**il comprend de plus l'étape consistant à envoyer un certificat numérique au système d'ordinateur activé par jeton de sécurité (105)

15. Procédé selon la revendication 11, **caractérisé en ce qu'**il comprend de plus l'étape consistant à inviter l'utilisateur à sélectionner une transaction d'authentification locale ou à distance.

16. Procédé selon la revendication 11, **caractérisé en ce qu'**il comprend de plus l'étape consistant à fournir à l'utilisateur une rétroaction sensorielle (205e) à partir d'au moins du système d'ordinateur activé par jeton de sécurité (105) représentative d'une transaction d'authentification à distance en cours.

17. Procédé selon la revendication 11, **caractérisé en ce que** la connexion de communications sécurisées sans fil est associée à un canal de communications dédié (220w) qui empêche d'établir des connexions de communications sécurisées sans fil concourantes avec le jeton de sécurité (75).

18. Procédé selon la revendication 16, **caractérisé en ce que** la rétroaction sensorielle (205e) comprend une rétroaction visuelle, tactile, auditive ou vibratoire.

19. Procédé selon la revendication 11, **caractérisé en ce que** la connexion de communications sécurisées sans fil est uniquement disponible lorsque le jeton de sécurité (75) est à l'intérieur d'une plage prédéfinie provenant du système d'ordinateur activé par jeton de sécurité (105).

20. Système pour établir une connexion de communications sécurisées de bout en bout entre un système d'ordinateur activé par jeton de sécurité (105) et un jeton de sécurité (75) associé à un dispositif intelligent sans fil situé à distance (110) comprenant :

un système d'ordinateur activé par jeton de sécurité (105) comprenant :

un système d'ordinateur activé par jeton de sécurité (105) comprenant :
des premiers moyens de transaction de sécurité pour au moins authentifier le jeton de sécurité (75) au système d'ordinateur activé par jeton de sécurité (105) ;
des premiers moyens de connexion de communications sécurisées pour au moins établir une connexion de communications sécurisées entre le système d'ordinateur activé par jeton de sécurité (105) et le jeton de sécurité (75) ; dans lequel
le dispositif intelligent situé à distance (110) comprend :

des moyens d'interface de jeton de sécurité (70r) pour relier au moins opérationnellement le jeton de sécurité (75) au dispositif intelligent situé à distance (110) ;
des moyens d'interface utilisateur (85r) pour au moins recevoir et acheminer un paramètre de sécurité critique (235) fourni par l'utilisateur aux moyens dudit interface de jeton de sécurité (70r) :

le jeton de sécurité (75) comprenant :

des seconds moyens de connexion de communications sécurisées pour établir au moins ladite connexion de communications sécurisées en association avec les premiers moyens de connexion de communications sécurisées;
des moyens de canal de communication dédié (220w) pour empêcher d'établir une connexion de communications sécurisées concourantes avec le jeton de sécurité (75) ; et

des seconds moyens de transaction de sécurité pour au moins authentifier l'utilisateur au jeton de sécurité (75), après la première transaction de sécurité, en utilisant au moins le paramètre de sécurité critique (235) ;
caractérisé en ce que le système comprend des moyens pour activer les moyens d'interface utilisateur (85r) pour recevoir et acheminer le paramètre de sécurité critique (235), lorsque les premiers moyens de connexion de communications sécurisées ont établi la connexion de communications sécurisées ;
et **en ce que** le système comprend des moyens pour transmettre un signal de résultat affirmatif en provenance du jeton de sécurité (75) au système d'ordinateur activé par jeton de sécurité (105) via la connexion de communications sécurisées de bout en bout si l'utilisateur est authentifié.

21. Système selon la revendication 20 dans lequel le système d'ordinateur activé par jeton de sécurité (105) est en communication sans fil avec le dispositif intelligent situé à distance (110) et le jeton de sécurité couplé de manière opérationnelle (75).

22. Système selon la revendication 20 dans lequel les premiers moyens de transaction de sécurité comprennent des moyens de protocole challenge/réponse et des moyens de cryptographie asymétrique.

23. Système selon la revendication 20, dans lequel les premiers moyens de connexion de communications sécurisées comprennent des moyens de création d'un ensemble de clés symétriques et des moyens d'échange de clés symétriques sécurisés.

24. Système selon la revendication 20, dans lequel les moyens d'interface de jeton de sécurité (70r) comprennent des moyens de communications de jeton de sécurité et des moyens de transfert de puissance électromagnétique.

25. Système selon la revendication 20, dans lequel les moyens de canal de communications dédié (220w) comprennent des moyens d'identification de canal unique qui sont accessibles par le système d'ordinateur activé par jeton de sécurité (105).

26. Système selon la revendication 20, dans lequel une exécution avec succès des premiers moyens de transaction de sécurité établit un premier état de sécurité du système d'ordinateur associé au client activé par le jeton de sécurité (75).

27. Système selon la revendication 20, dans lequel l'établissement de la connexion de communications sécurisées établit un premier état de sécurité de jeton associé au jeton de sécurité (75).

28. Système selon la revendication 20, dans lequel l'exécution avec succès des seconds moyens de transaction de sécurité établit un second état de sécurité de jeton (75) associé au jeton de sécurité (75).

29. Système selon la revendication 20, dans lequel le système d'ordinateur activé par jeton de sécurité (105) comprend de plus des moyens de détection de proximité (115c).

30. Système selon la revendication 20, dans lequel :

le système d'ordinateur activé par jeton de sécurité (105) comprend :

un premier processeur (5c) ;
une première mémoire (10c) reliée au premier processeur (5c) ;
au moins une application d'authentification à distance mémorisée de manière opérationnelle dans une première partie de la première mémoire ayant des instructions logiques exécutables par le premier processeur (5c) pour ;
effectuer l'authentification du jeton de sécurité (75) ;
établir une connexion de communications sécurisées avec le jeton de sécurité (75);

le dispositif intelligent situé à distance (110) comprenant ;
un second processeur (5r) ;
une seconde mémoire (10r) reliée au second processeur (5r) ; une interface de jeton de sécurité (70r) reliée au second processeur (5r)
une interface utilisateur (85r) reliée au second processeur (5r) ; et
au moins une application d'interface de dispositif situé à distance mémorisée de manière opérationnelle dans une partie de la seconde mémoire (10r) ayant des instructions logiques exécutables par le second processeur (5r) pour :

émuler une interface de dispositif à jeton de sécurité reliée localement à au moins un système d'ordinateur activé par jeton de sécurité (105) ; et
recevoir et acheminer de manière conditionnelle le paramètre de sécurité critique (235) fourni par l'utilisateur via l'interface utilisateur (85r) du/au jeton de sécurité (75) ; et

le jeton de sécurité (75) comprenant :

au moins un troisième processeur (5t) ;
une troisième mémoire reliée audit au moins un troisième processeur (5t) ;
une interface de communications et de puissance électromagnétique reliée au dit au moins un troisième processeur (5t) et à l'interface de jeton de sécurité (70r) ;
au moins une application d'authentification à distance de jeton mémorisée de manière opérationnelle dans une seconde partie de la troisième mémoire ayant des instructions logiques exécutables par le au moins un troisième processeur (5t) pour :

établir la connexion de communications sécurisées avec le système d'ordinateur activé par jeton de sécurité (105) ;
limiter la connexion de communications sécurisées à un canal de communications sans fil unique ; et
effectuer l'authentification de l'utilisateur sur la base au moins en partie du paramètre de sécurité critique (235).

31. Système selon la revendication 30, comprenant de plus un premier émetteur récepteur sans fil (60c) relié fonctionnellement au premier processeur (5c) dans un traitement de communications avec un second émetteur récepteur sans fil (60r) relié fonctionnellement au second processeur (5r).

32. Système selon la revendication 30, comprenant de plus une clé publique (225c) associée au jeton de sécurité (75) mémorisée de manière récupérable dans une seconde partie de la première mémoire (10c) et une clé privée (230) mémorisée de manière récupérable dans une seconde partie de la troisième mémoire, la clé privée (230) étant une contrepartie de la clé publique (225 C).

33. Système selon la revendication 30, comprenant de plus un paramètre de sécurité critique de référence (235r) mémorisé de manière récupérable dans une troisième partie de la troisième mémoire.

34. Système selon la revendication 32, dans lequel lesdites clés publique (225c) et privée (230) sont incorporées dans le protocole de challenge/réponse utilisé pour authentifier le jeton de sécurité (75) au système d'ordinateur activé par jeton de sécurité (105).

35. Système selon la revendication 34, dans lequel ladite au moins une application d'authentification à distance comprend de plus des instructions logiques exécutables par le premier processeur (5c) pour produire un ensemble de clés symétriques (285t, 285s) et effectuer un échange de clés sécurisé avec le jeton de sécurité (75).

36. Système selon la revendication 35, dans lequel l'échange de clés sécurisé est effectué en utilisant des clés publiques (225c) et privées (230).

37. Système selon la revendication 35 dans lequel l'ensemble de clés symétriques (285t, 285s) est incorporé dans la connexion de communications sécurisées de bout en bout.

38. Système selon la revendication 30, dans lequel l'utilisateur est authentifié par la au moins une application d'authentification à distance de jeton en comparant le paramètre de sécurité critique fourni (235) au paramètre de sécurité critique de référence (235r).

39. Système selon la revendication 30, dans lequel la au moins une application d'authentification à distance de jeton restreint l'utilisation de la connexion de communications sécurisées de bout en bout jusqu'à ce que l'utilisateur soit authentifié.

40. Système selon la revendication 30, dans lequel la connexion de communications sécurisées de bout en bout est restreinte à une connexion sans fil unique avec le jeton de sécurité (75) en utilisant un canal de communications dédié (220w) commandé par la au moins une application d'authentification à distance de jeton.

41. Système selon la revendication 36, dans lequel le canal de communications dédié (220w) comprend un identificateur unique disponible par le système d'ordinateur activé par jeton de sécurité (105).

42. Système selon la revendication 30, dans lequel l'interface de communications et de puissance électromagnétique comprend des moyens inductifs, des moyens capacitifs ou des moyens de contact électrique.

43. Programme d'ordinateur mis en oeuvre sous une forme tangible pouvant être lue par un processeur à jeton de sécurité (5t), dans lequel le programme d'ordinateur comprend des instructions exécutables mémorisées sur celui-ci pour mettre en oeuvre le procédé de la revendication 1.

44. Programme d'ordinateur selon la revendication 43, dans lequel la forme tangible comprend des supports magnétiques, supports optiques, ou supports logiques.

45. Programme d'ordinateur selon la revendication 43, dans lequel les instructions exécutables sont mémorisées dans un format de code comprenant un code à octets, compilé, interprété, compilable et interprétable.

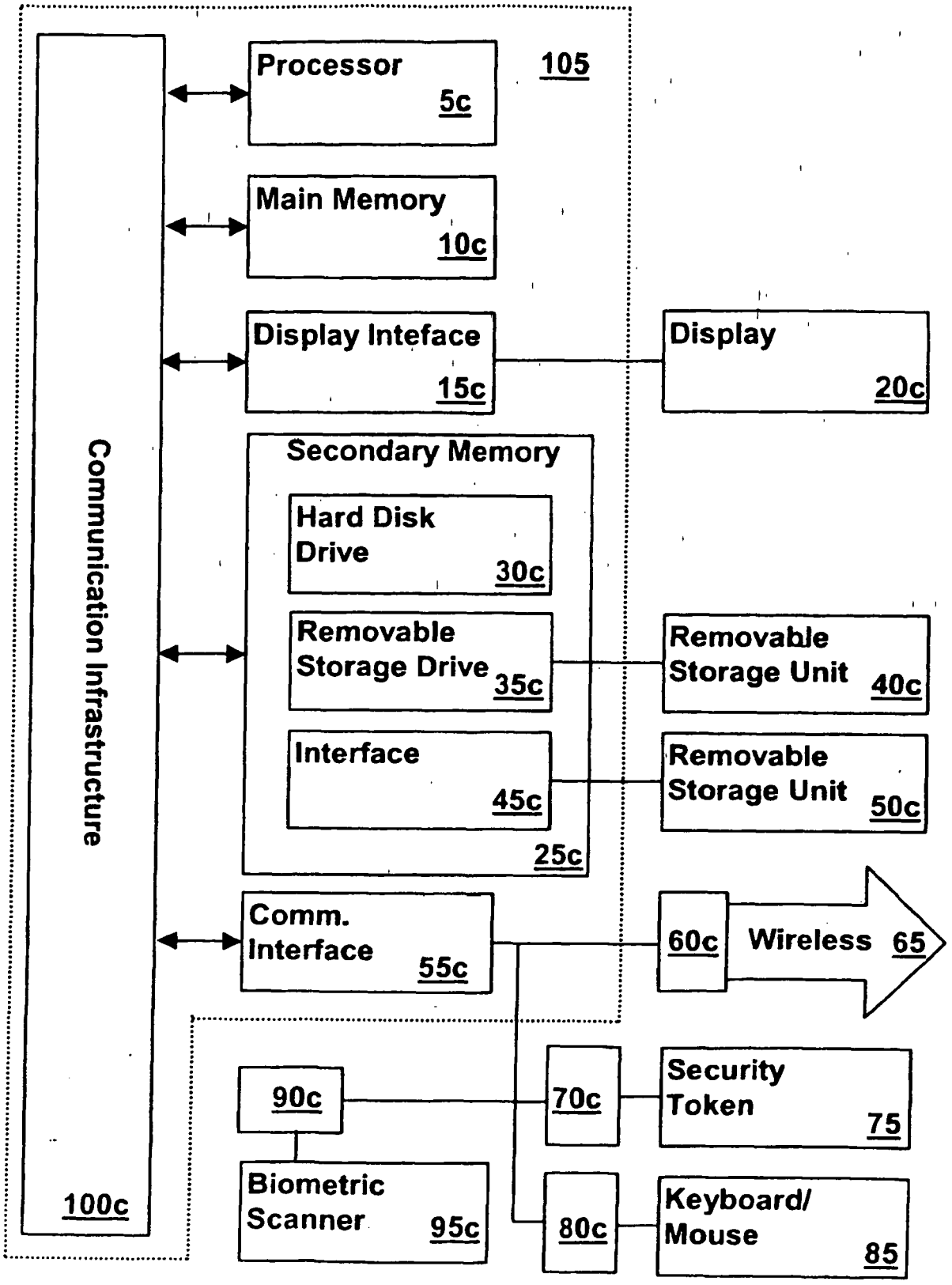
Processor
5c
105
Main Memory
10c
Display Inteface
15c
Display
20c
Secondary Memory
Hard Disk Drive
30c
Removable Storage Drive
35c
Removable Storage Unit
40c
Interface
45c
Removable Storage Unit
50c
25c
Comm. Interface
55c
60c
Wireless
65
Communication Infrastructure
100c
90c
70c
Security Token
75
Biometric Scanner
95c
80c
Keyboard/ Mouse
85

FIG. 1

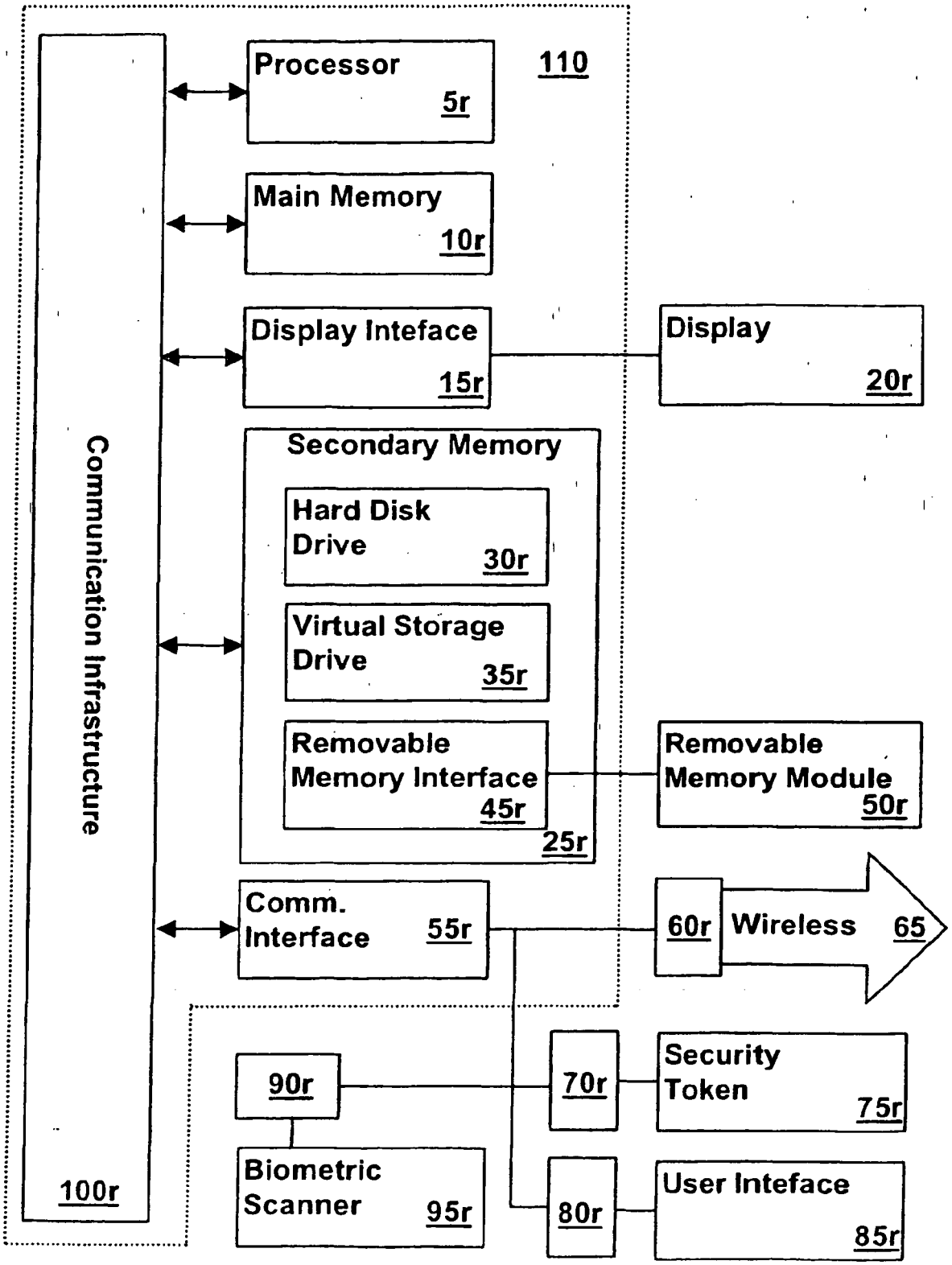
Processor
5r
110
Main Memory
10r
Display Inteface
15r
Display
20r
Secondary Memory
Hard Disk Drive
30r
Virtual Storage Drive
35r
Removable Memory Interface
45r
25r
Removable Memory Module
50r
Comm. Interface
55r
60r
Wireless
65
Communication Infrastructure
100r
90r
70r
Security Token
75r
Biometric Scanner
95r
80r
User Inteface
85r

FIG. 1A

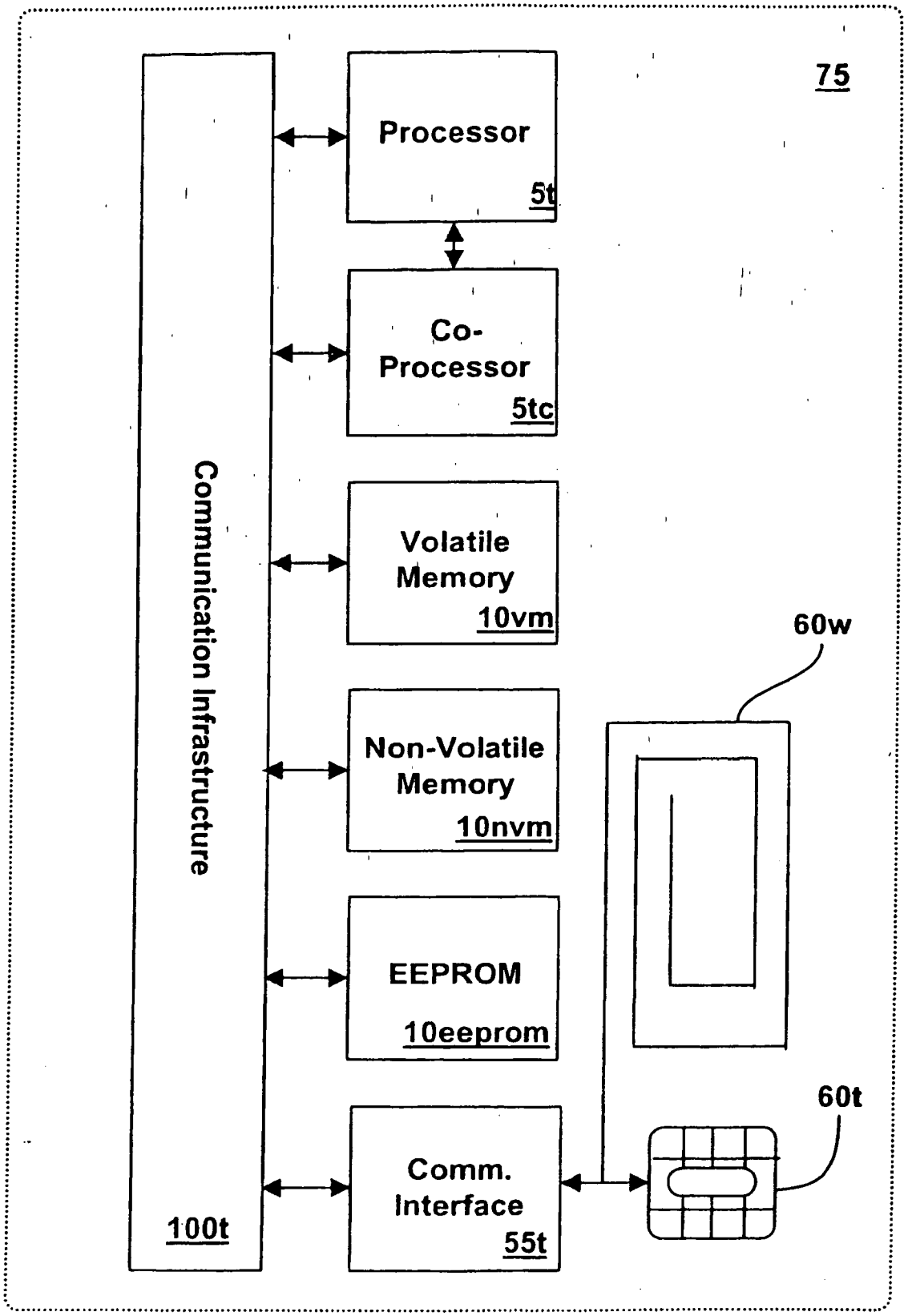
75
Processor
5t
Co-
Processor
5tc
Volatile
Memory
10vm
Non-Volatile
Memory
10nvm
EEPROM
10eeprom
Comm.
Interface
55t
Communication Infrastructure
100t
60w
60t

FIG. 1B

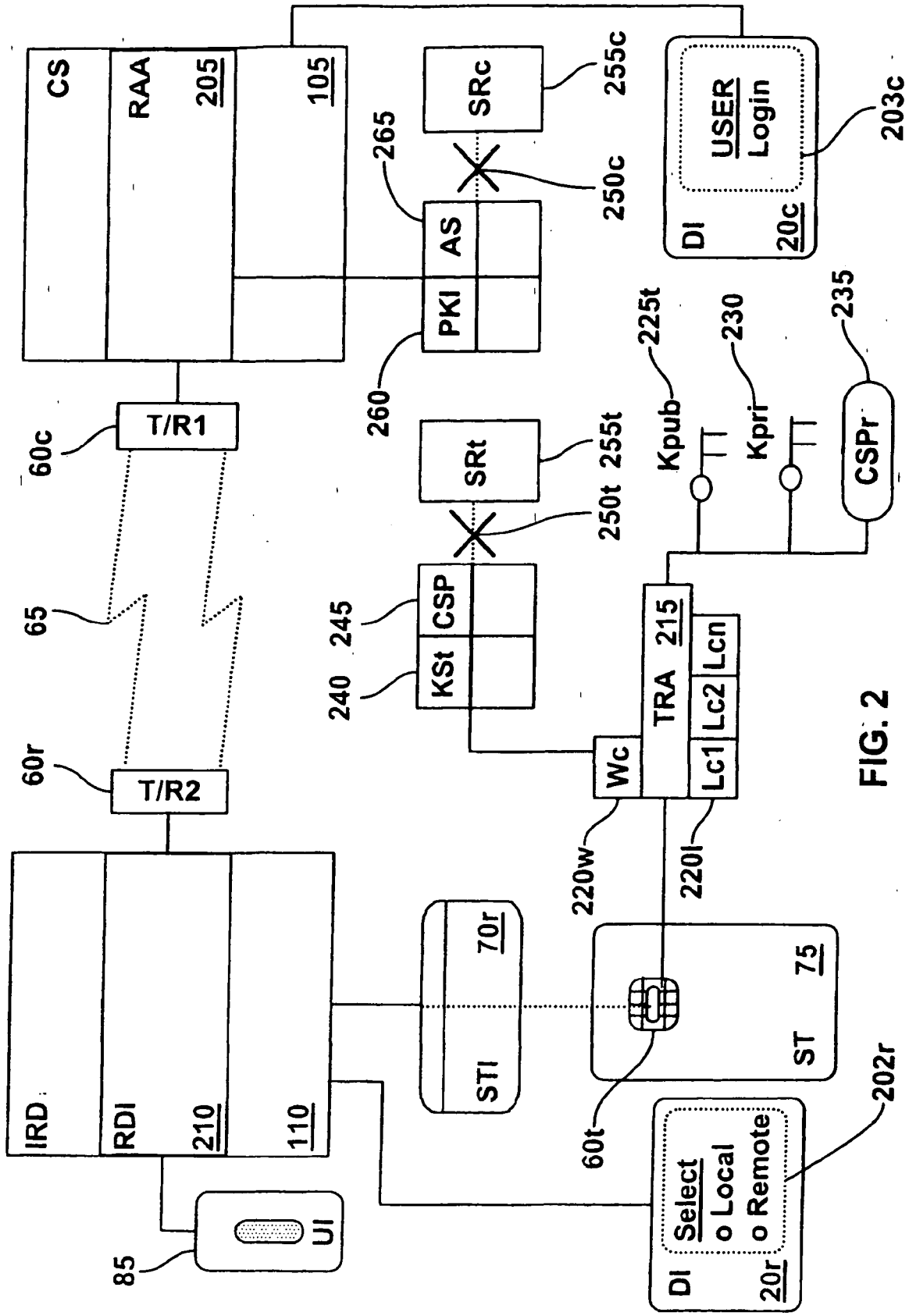
CS
RAA
205
105
SRc
255c
265
250c
AS
PKI
260
USER
Login
203c
DI
20c
60c
T/R1
SRt
255t
250t
Kpub
225t
Kpri
230
CSPr
235
65
245
CSP
KSt
240
TRA
215
Lcn
Lc2
Lc1
Wc
60r
T/R2
220w
220l
IRD
RDI
210
110
70r
STI
75
ST
60t
202r
Select
o Local
o Remote
DI
20r
UI
85

FIG. 2

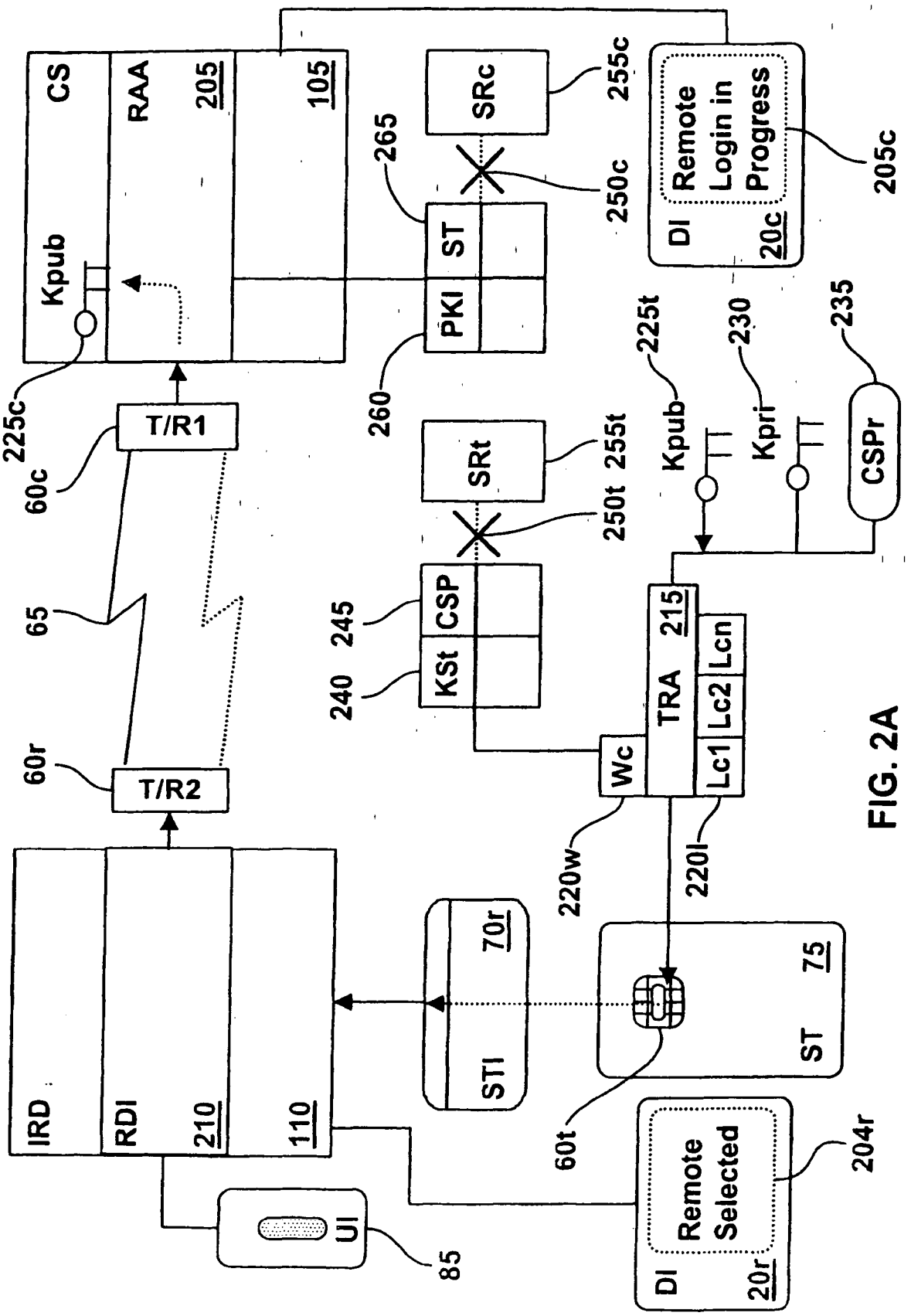
CS
RAA
205
105
Kpub
225c
60c
T/R1
65
60r
T/R2
IRD
RDI
210
110
UI
85
SRc
255c
250c
265
ST
PKI
260
DI
Remote Login in Progress
20c
205c
SRt
255t
250t
240
245
CSP
KSt
225t
Kpub
230
Kpri
235
CSPr
TRA
215
Wc
Lcn
Lc2
Lc1
220w
220l
70r
STl
60t
ST
75
DI
Remote Selected
20r
204r

FIG. 2A

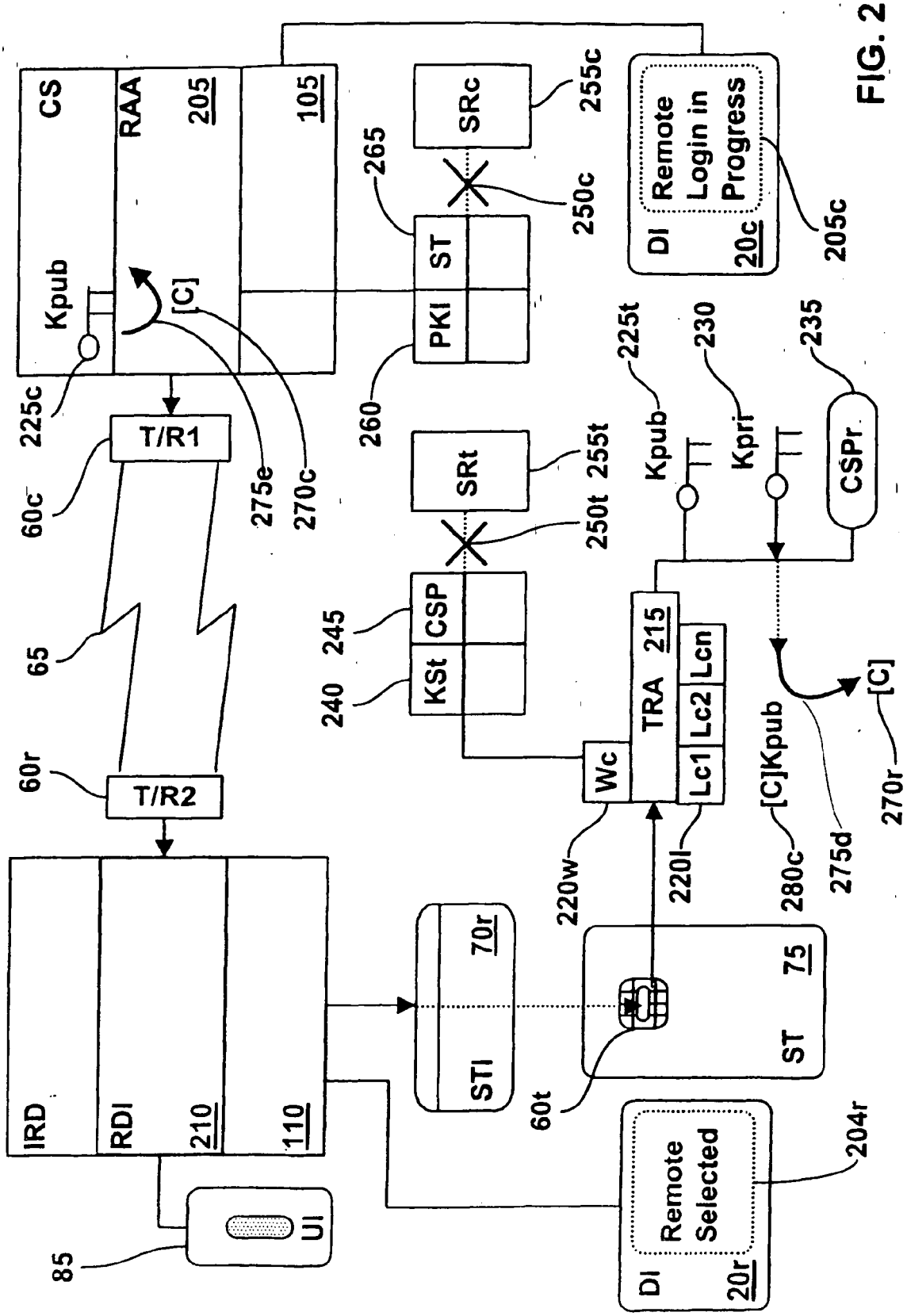
CS
RAA
205
105
Kpub
[C]
225c
60c
T/R1
65
60r
T/R2
IRD
RDI
210
110
UI
85
275e
270c
265
ST
PKI
260
SRc
255c
250c
DI
Remote Login in Progress
20c
205c
SRt
255t
250t
CSP
KSt
245
240
225t
Kpub
230
Kpri
235
CSPr
TRA
215
Lcn
Lc2
Lc1
Wc
220w
220l
[C]Kpub
280c
275d
[C]
270r
70r
STl
60t
ST
75
Remote Selected
DI
20r
204r

FIG. 2B

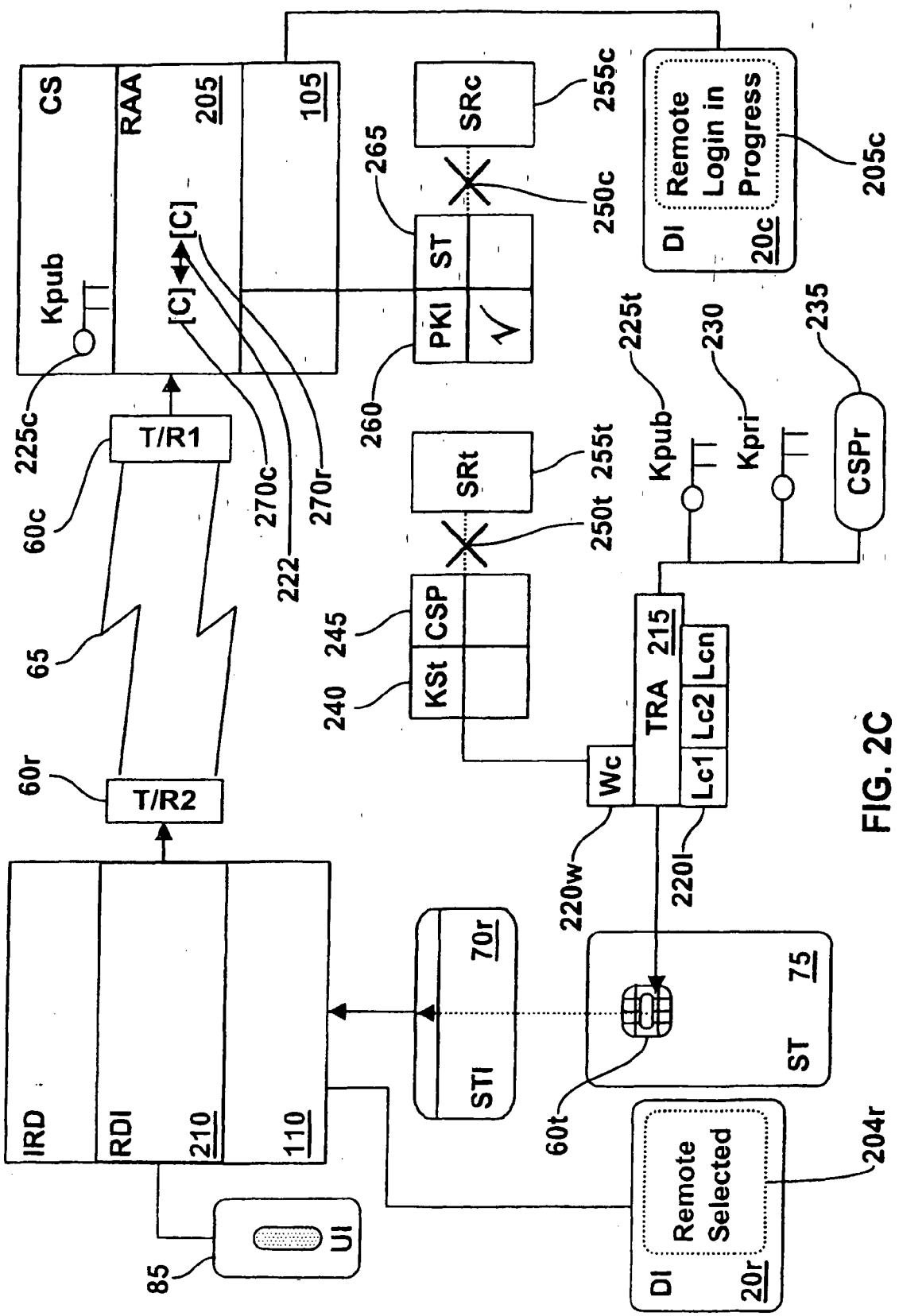
CS
RAA
205
105
Kpub
[C]
[C]
225c
60c
T/R1
65
60r
T/R2
IRD
RDI
210
110
85
UI
270c
222
270r
SRc
255c
250c
265
ST
PKI
260
SRt
255t
250t
245
CSP
240
KSt
DI
Remote Login in Progress
20c
205c
225t
Kpub
230
Kpri
235
CSPr
215
TRA
Lcn
Lc2
Lc1
Wc
220w
220l
70r
STI
ST
75
60t
DI
Remote Selected
20r
204r

FIG. 2C

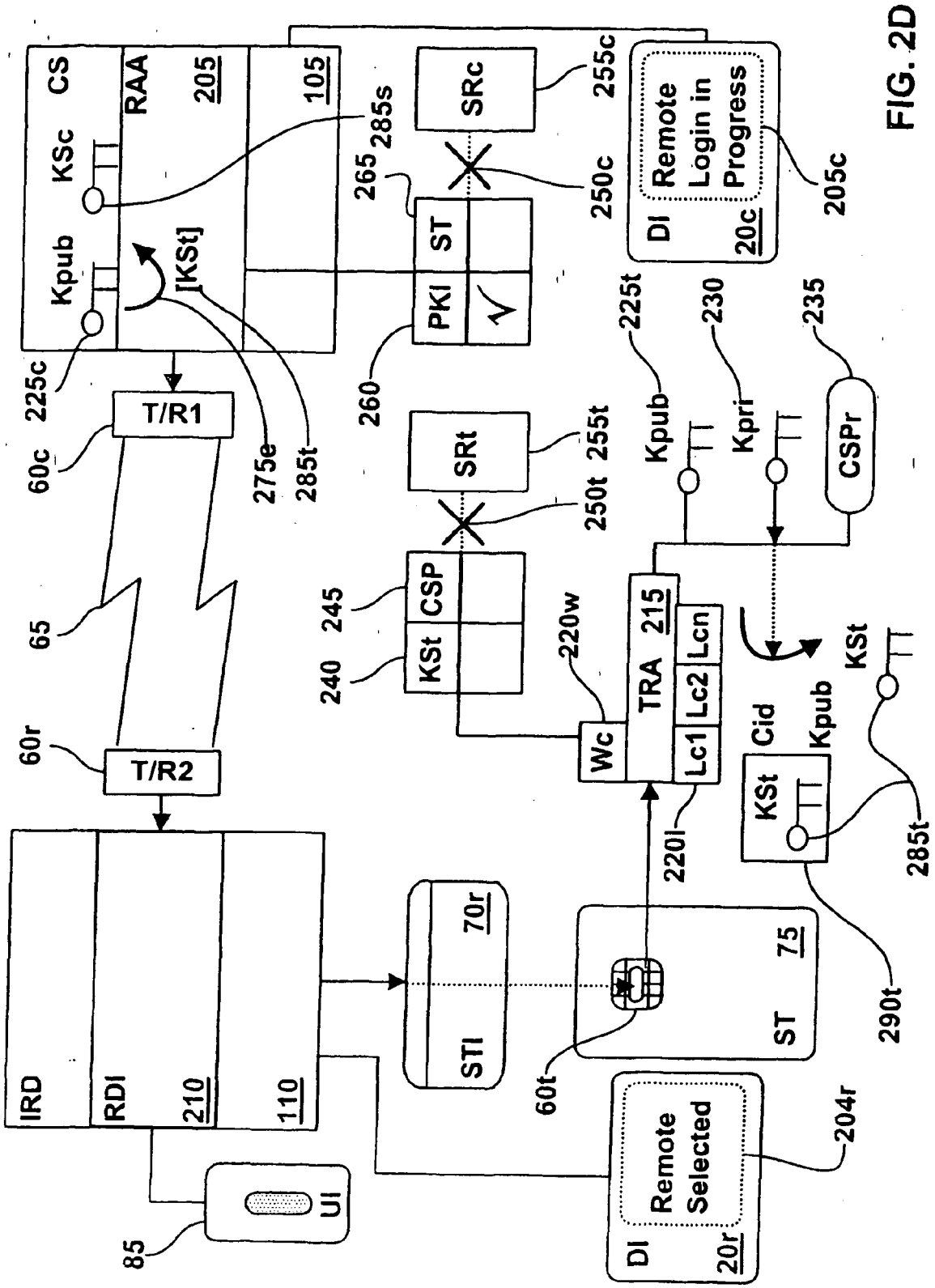
CS
RAA
205
105
KSc
Kpub
[KSt]
285s
225c
T/R1
60c
275e
285t
65
60r
T/R2
IRD
RDI
210
110
UI
85
265
ST
PKI
260
SRc
255c
250c
DI
Remote Login in Progress
20c
205c
SRt
255t
250t
CSP
KSt
245
240
225t
230
235
Kpub
Kpri
CSPr
220w
Wc
TRA
215
Lcn
Lc2
Lc1
220l
Cid
Kpub
KSt
KSt
285t
290t
70r
STl
75
ST
60t
DI
Remote Selected
20r
204r

FIG. 2D

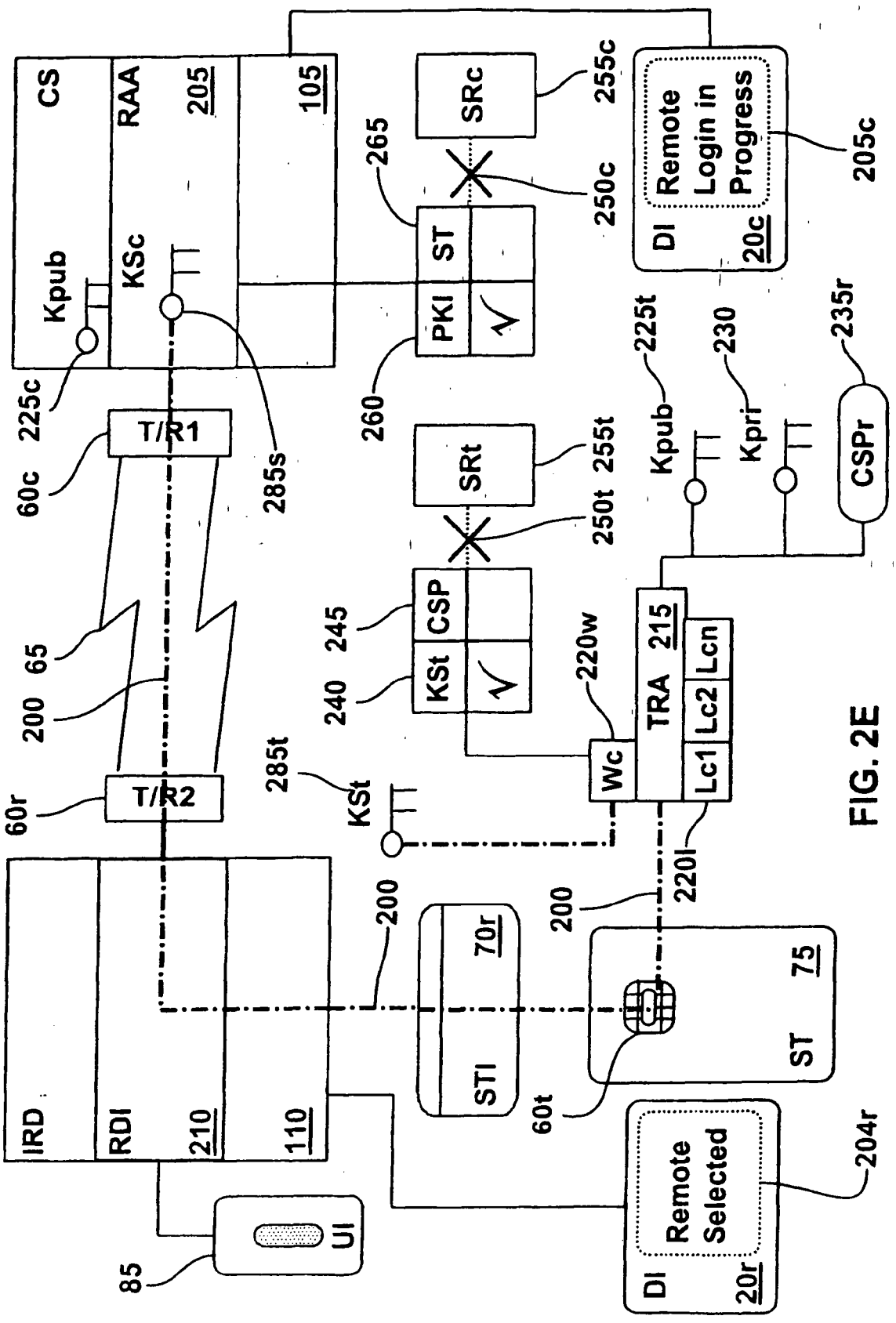
CS
RAA
205
105
Kpub
KSc
225c
60c
T/R1
285s
SRc
255c
265
250c
ST
PKI
260
Remote Login in Progress
DI
20c
205c
SRt
255t
250t
225t
230
235r
Kpub
Kpri
CSPr
245
CSP
KSt
240
220w
TRA
215
Lcn
Lc2
Lc1
Wc
65
200
60r
T/R2
285t
KSt
220l
200
70r
STl
60t
ST
75
IRD
RDI
210
110
85
UI
Remote Selected
DI
20r
204r

FIG. 2E

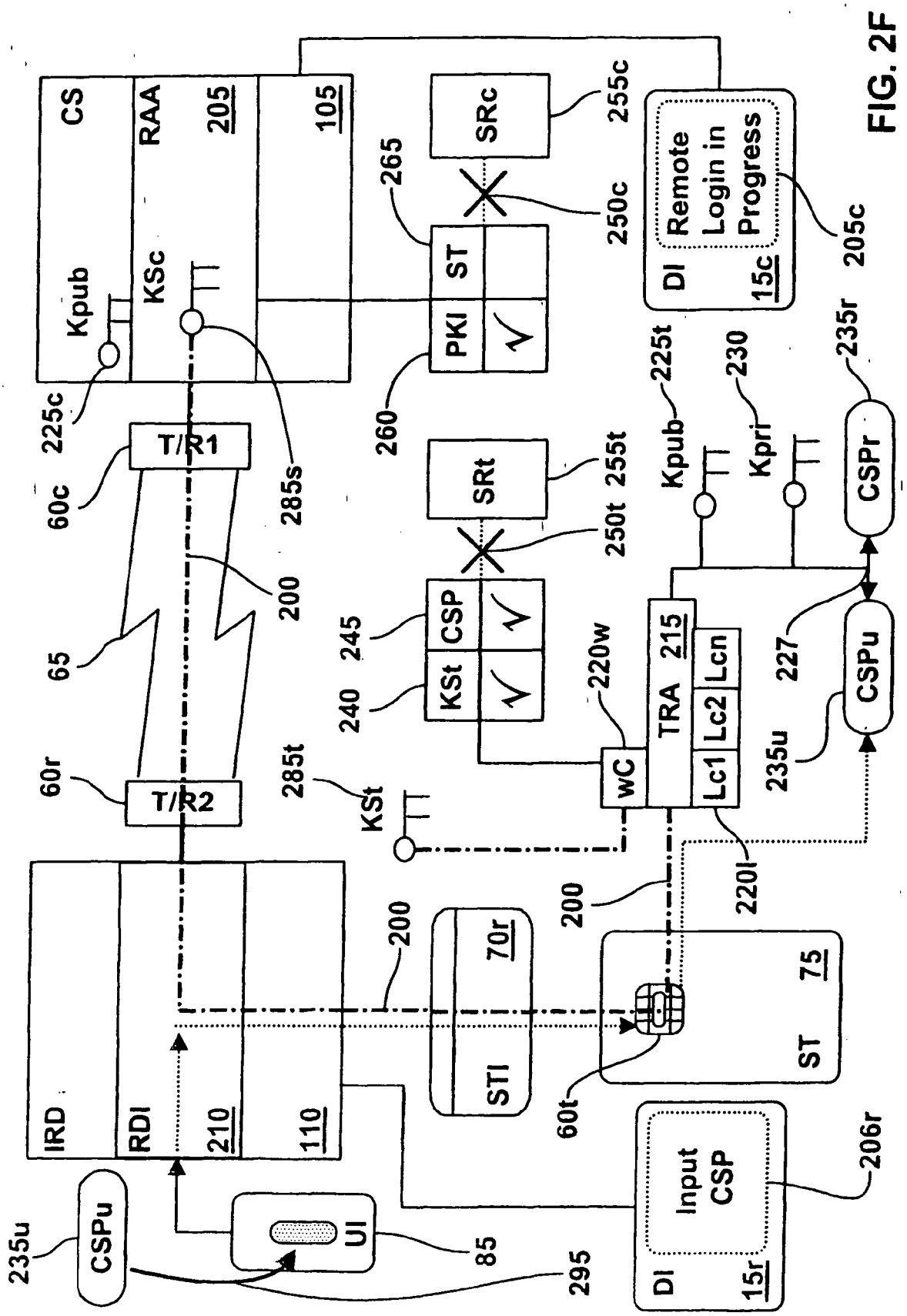
CS
RAA
205
105
Kpub
KSc
225c
60c
T/R1
285s
200
65
60r
T/R2
285t
KSt
IRD
RDI
210
110
200
235u
CSPu
UI
85
295
SRc
255c
250c
265
ST
PKI
260
SRt
255t
250t
CSP
KSt
245
240
220w
wC
TRA
215
Lcn
Lc2
Lc1
DI
Remote
Login in
Progress
15c
205c
225t
Kpub
230
Kpri
235r
CSPr
227
CSPu
235u
220l
200
70r
STI
60t
75
ST
DI
Input
CSP
15r
206r

FIG. 2F

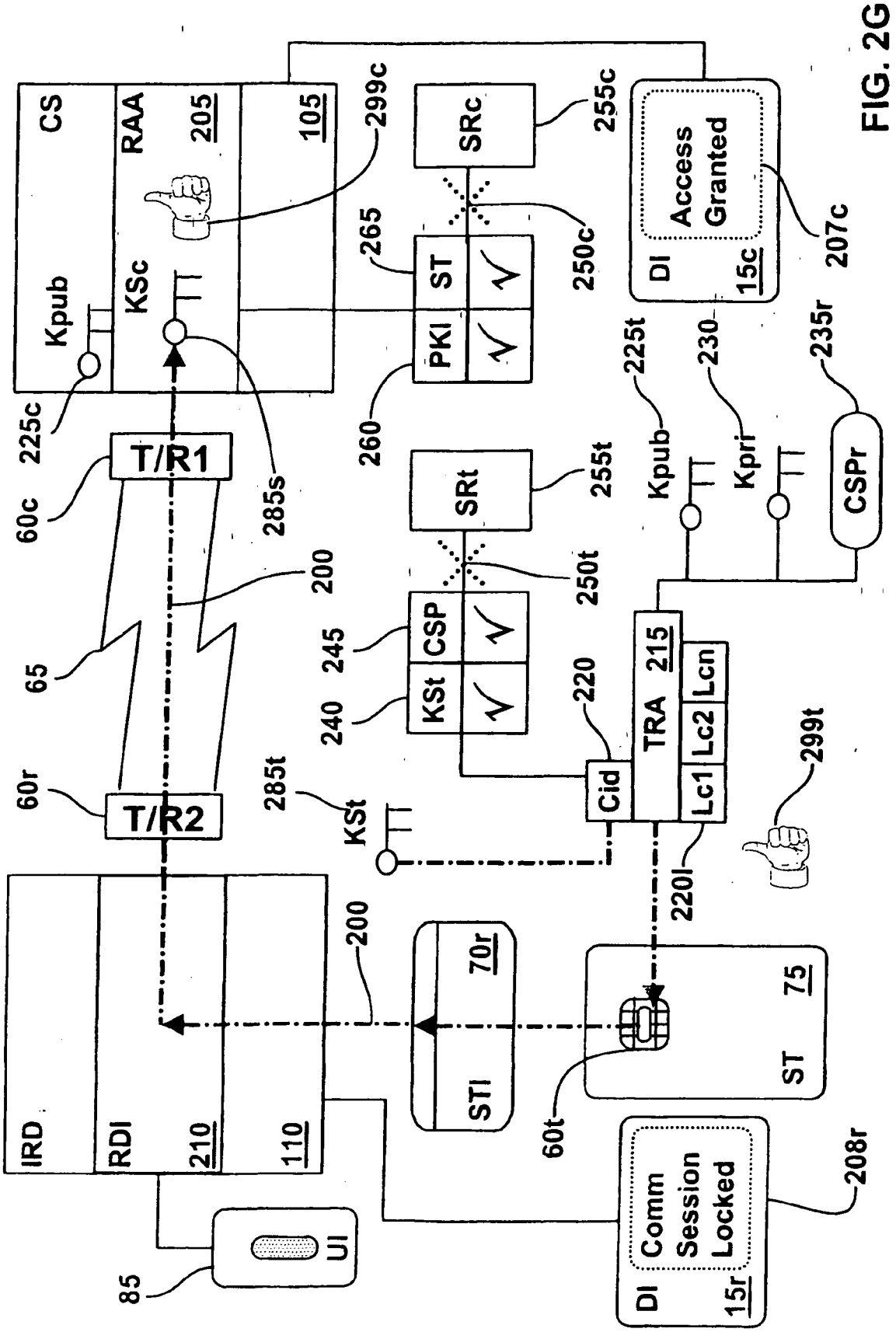
CS
RAA
205
105
299c
Kpub
KSc
225c
60c
T/R1
285s
SRc
255c
265
ST
PKI
250c
260
DI
Access Granted
15c
207c
225t
230
235r
Kpub
Kpri
CSPr
SRt
255t
250t
200
65
245
CSP
KSt
240
220
TRA
215
Cid
Lc1
Lc2
Lcn
60r
T/R2
285t
KSt
299t
220l
IRD
RDI
210
110
200
70r
STI
ST
75
60t
UI
85
DI
Comm Session Locked
15r
208r

FIG. 2G

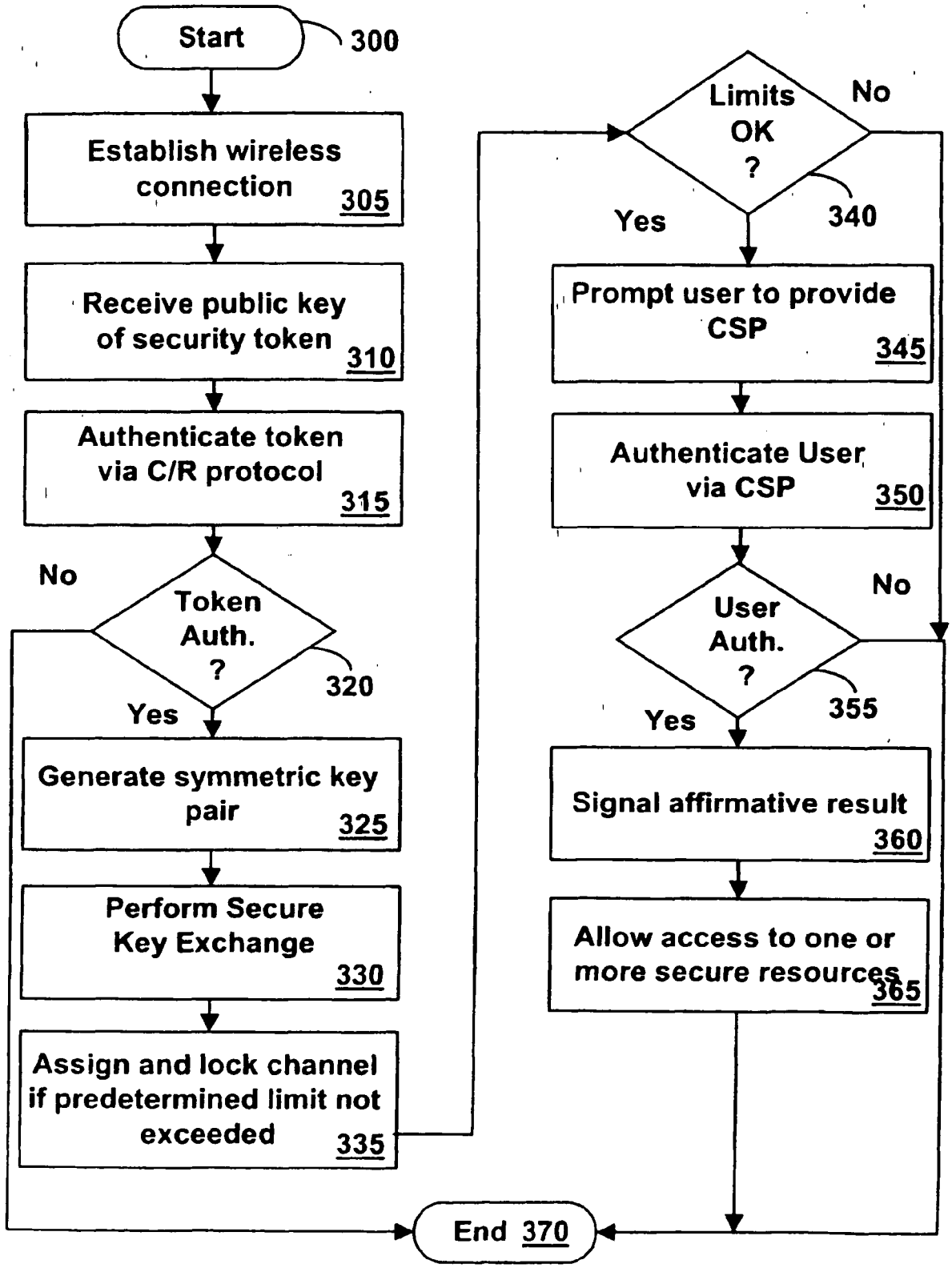
Start
300
Establish wireless connection
305
Receive public key of security token
310
Authenticate token via C/R protocol
315
Token Auth. ?
320
No
Yes
Generate symmetric key pair
325
Perform Secure Key Exchange
330
Assign and lock channel if predetermined limit not exceeded
335
Limits OK ?
340
No
Yes
Prompt user to provide CSP
345
Authenticate User via CSP
350
User Auth. ?
355
No
Yes
Signal affirmative result
360
Allow access to one or more secure resources
365
End 370

FIG. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 0733971 A **[0005]**
- US 5841868 A **[0006]**
- US 4945468 A **[0007]**
- US 20020095587 A1 **[0008]**
- US 6456958 B **[0048]**
- US 6307471 B **[0048]**
- US 6070240 A **[0048]**
- US 20020104012 A1 **[0048]**
- US 20020069030 A1 **[0048]**
- US 20020065625 A **[0048]**
- US 20020162021 A1 **[0066]**
- US 20040123152 A1 **[0068]**
- US 20040221174 A **[0069]**