Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2365856 C 2011/11/01

(11)(21) 2 365 856

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2000/04/07
(87) Date publication PCT/PCT Publication Date: 2000/10/19
(45) Date de délivrance/Issue Date: 2011/11/01
(85) Entrée phase nationale/National Entry: 2001/08/28
(86) N° demande PCT/PCT Application No.: US 2000/009323
(87) N° publication PCT/PCT Publication No.: 2000/062507
(30) Priorité/Priority: 1999/04/09 (US60/128,772)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01), *G06F 1/00* (2006.01), *G06F 21/00* (2006.01), *H04L 9/32* (2006.01), *H04M 7/00* (2006.01), *G06F 12/14* (2006.01)

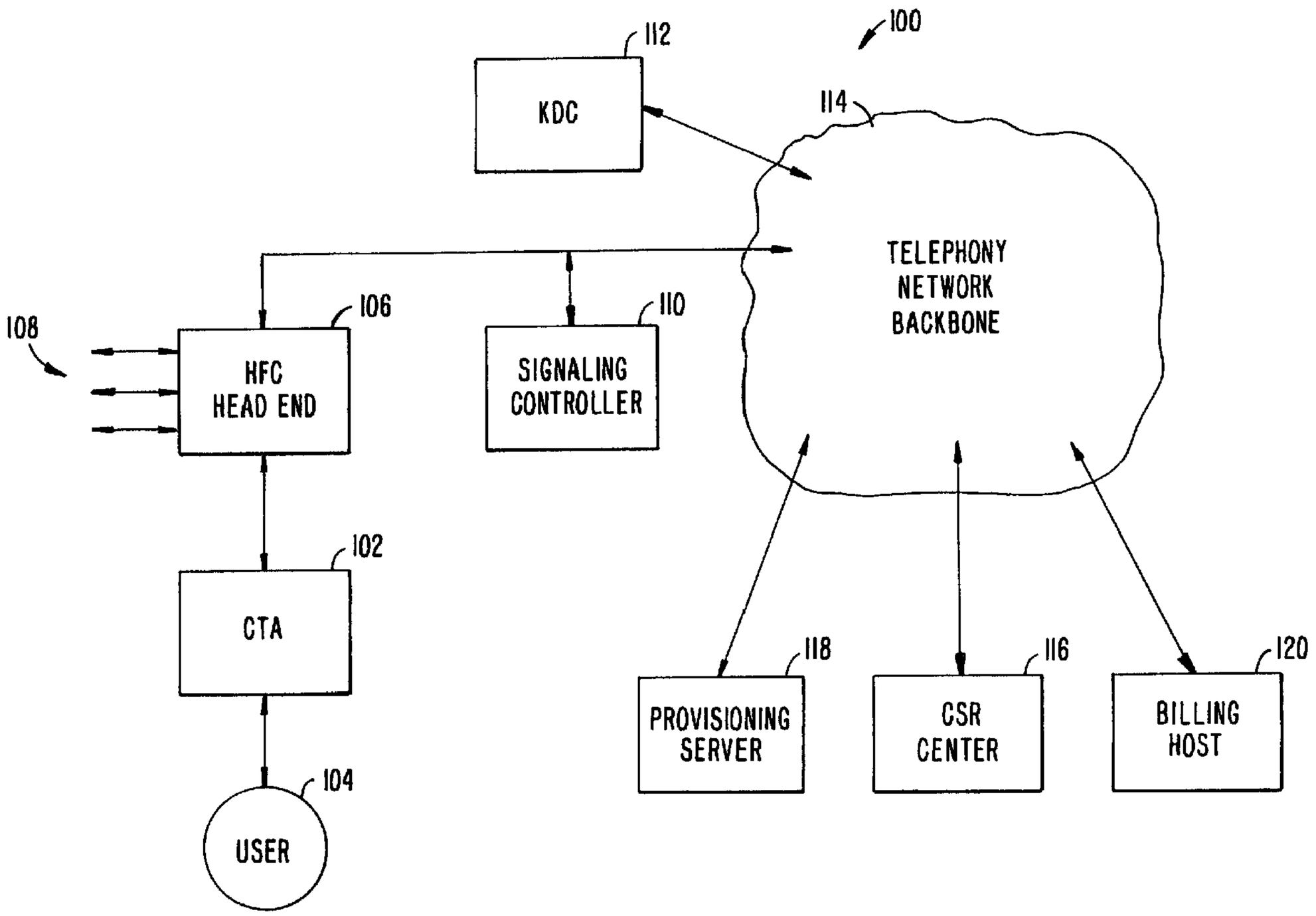
(72) Inventeur/Inventor:
MEDVINSKY, SASHA, US

(73) Propriétaire/Owner:
GENERAL INSTRUMENT CORPORATION, US

(74) Agent: FETHERSTONHAUGH & CO.

(54) Titre : GESTION DES CLES ENTRE UN ADAPTATEUR DE TELEPHONIE PAR CABLE ET UN SIGNALEUR ASSOCIE

(54) Title: KEY MANAGEMENT BETWEEN A CABLE TELEPHONY ADAPTER AND ASSOCIATED SIGNALING CONTROLLER



(57) Abrégé/Abstract:
A highly scalable key management architecture for secure client-server systems used in IP telephony network, wherein cryptographic state needs to be saved only by the clients. This architecture takes advantage of existing key management protocols,

CA 2365856 C 2011/11/01

(11)(21) 2 365 856

(13) C

(57) Abrégé(suite)/Abstract(continued):
Kerberos with the PKINIT (public key) extension, to provide an IP telephony system having a high degree of scalability. In the case of lost security associations, the architecture provides for lightweight rekeying operations that allow clients to quickly re-establish the lost association or switch to a different server. The key management architecture includes a method for establishing a secure channel between an IP telephony endpoint and Server in an IP telephony network. The endpoint is coupled to a user and the Server is coupled to the IP telephony network. The method comprises steps of transmitting from the endpoint to a key distribution center a request for a security ticket, receiving the security ticket from the key distribution center, transmitting from the endpoint to the Server a request for a sub-key, receiving the sub-key from the Server, and establishing a secure channel between the endpoint and the Server using the sub-key.

CA 02365856 2001-08-28

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 29/06, H04M 7/00

A1

(11) International Publication Number: **WO 00/62507**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/US00/09323

(22) International Filing Date: 7 April 2000 (07.04.00)

(30) Priority Data:
60/128,772 9 April 1999 (09.04.99) US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

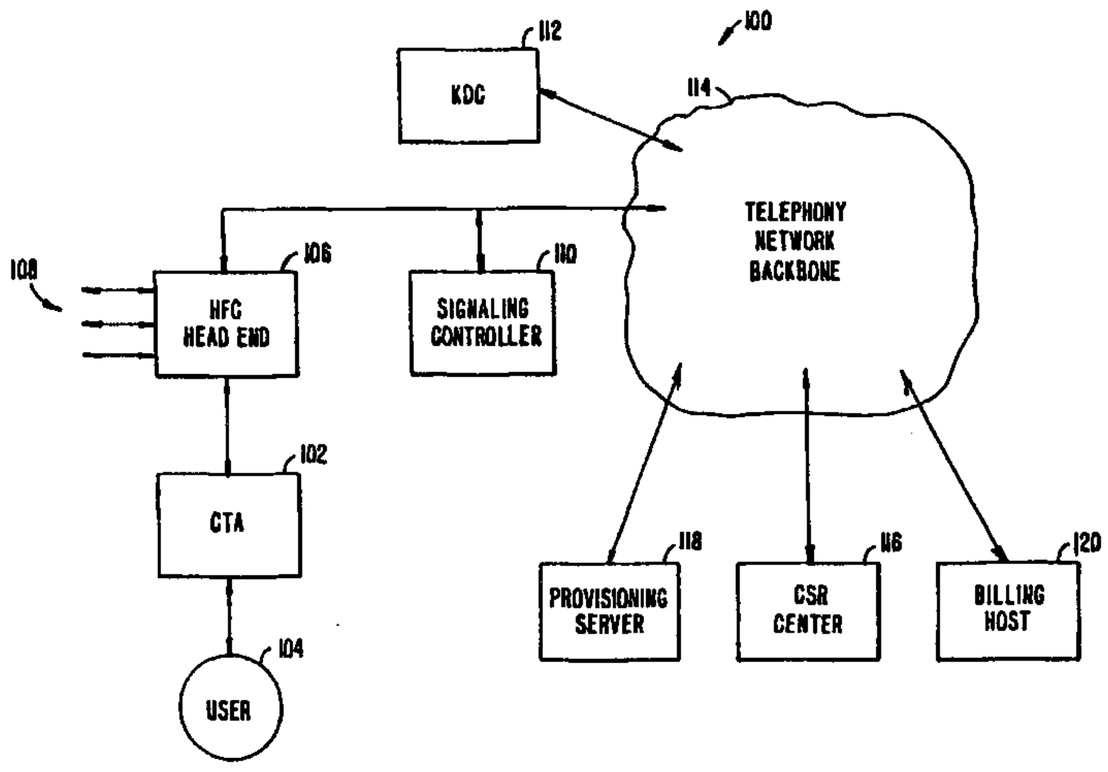
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MEDVINSKY, Sasha [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US).

(74) Agents: TAGLIAFERRI, Daniel, D. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: KEY MANAGEMENT BETWEEN A CABLE TELEPHONY ADAPTER AND ASSOCIATED SIGNALING CONTROLLER



(57) Abstract

A highly scalable key management architecture for secure client–server systems used in IP telephony network, wherein cryptographic state needs to be saved only by the clients. This architecture takes advantage of existing key management protocols, Kerberos with the PKINIT (public key) extension, to provide an IP telephony system having a high degree of scalability. In the case of lost security associations, the architecture provides for lightweight rekeying operations that allow clients to quickly re–establish the lost association or switch to a different server. The key management architecture includes a method for establishing a secure channel between an IP telephony endpoint and Server in an IP telephony network. The endpoint is coupled to a user and the Server is coupled to the IP telephony network. The method comprises steps of transmitting from the endpoint to a key distribution center a request for a security ticket, receiving the security ticket from the key distribution center, transmitting from the endpoint to the Server a request for a sub–key, receiving the sub–key from the Server, and establishing a secure channel between the endpoint and the Server using the sub–key.

KEY MANAGEMENT BETWEEN A CABLE TELEPHONY ADAPTER AND ASSOCIATED SIGNALING CONTROLLER

FIELD OF THE INVENTION

This invention relates generally to secure communication based on key management in Client-Server systems, and more particularly, to a scalable key management system for use in IP telephony networks.

BACKGROUND OF THE INVENTION

In an Internet Protocol (IP) telephony network, a network server may be responsible for setting up phone calls with up to 100,000 clients. The clients may be coupled to the telephony network via cable telephony adapter (CTA) devices. In order to secure call signaling, an Internet Protocol Security (IPSec) association is set up between each client and the server. This has to be done in a timely fashion to minimize the CPU overhead at the server and to minimize the call setup delay.

In order to handle large numbers of clients, key management needs to be as fast as possible. For example, security associations might be lost when a server goes down or become too busy to handle all of its clients. The lost security associations must then be re-established again when needed. Manual administration of clients is unsuitable because of the high overhead costs and lack of scalability. Other techniques used in architectures unrelated to IP telephony are also not suitable, since they do not provide the desired scalability and low administration overhead.

SUMMARY OF THE INVENTION

The present invention includes a highly scalable key management architecture for secure client-server systems used in an IP telephony network, wherein cryptographic state needs to be saved only by the clients. This architecture takes advantage of existing key management protocols, Kerberos with the PKINIT (public key) extension, to provide an IP telephony system having a high degree of scalability. In the case of lost security associations, the architecture provides for lightweight

rekeying operations that allow clients to quickly re-establish the lost association or switch to a different server.

In accordance with one aspect of the invention, there is provided a secure IP telephony system. The system includes a signaling controller within an IP telephony network and in communication with at least one Cable Telephony Adapter (CTA), and configured to generate a symmetric sub-key in response to a request from the at least one CTA. The request includes a signaling controller ticket comprising a signaling controller session key, an identity of the at least one CTA, and an identity of the signaling controller. The signaling controller is further configured to distribute the symmetric sub-key to the at least one CTA in response to the signaling controller ticket. The signaling controller further includes a Key Distribution Center (KDC) within the IP telephony network and coupled to the signaling controller, and configured to generate and distribute the signaling controller ticket and the signaling controller session key to the at least one CTA using public key encryption. The at least one CTA generates an additional symmetric key specific for a given call based on the symmetric sub-key provided by the signaling controller that is utilized for the given call for CTA to CTA signaling or bearer channel communication.

The signaling controller may be configured to generate and distribute the symmetric sub-key in response to a Kerberos request from the at least one CTA.

The signaling controller may distribute the sub-key encrypted with the signaling controller session key.

The signaling controller may receive from the at least one CTA the signaling controller ticket, wherein a portion of the signaling controller ticket may be encrypted with a signaling controller server key.

The request may comprise a Kerberos Application Request having the signaling controller ticket and encrypted data including a name of the at least one CTA.

The request may include a timestamp.

The signaling controller may authenticate the at least one CTA using the signaling controller ticket.

The signaling controller may communicate with the CTA in an IPsec ESP session in response to receiving a valid signaling controller ticket.

The KDC may generate and distribute the signaling controller ticket in a Kerberos exchange with the at least one CTA.

The system may further include a Provisioning Certificate Authority (CA) in communication with the IP telephony network configured to receive a manufacturer signed CTA certificate and distribute an operator network-specific certificate to the at least one CTA.

The signaling controller ticket may include a Kerberos ticket.

The signaling controller ticket may further include an expiration time.

The KDC may distribute to the at least one CTA the signaling controller ticket and a copy of the session key outside of the signaling controller ticket encrypted with a CTA public key.

The KDC may distribute the signaling controller ticket to the at least one CTA, and may also distribute to the at least one CTA a copy of the session key outside of the signaling controller ticket encrypted using a shared secret derived from a Diffie-Hellman exchange.

The additional symmetric key may be valid for a single call.

A further understanding of various aspects, features and advantages of the invention disclosed herein may be realized by reference to the specific embodiments described in the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a telephony network constructed in accordance with the present invention;

FIG. 2 shows message exchange diagram for establishing a secure communication channel in accordance with the present invention; and

FIG. 3 shows a method for establishing a secure communication channel using the messages shown in FIG. 2.

DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

Embodiments of the present invention provide for establishing a secure channel between an IP telephony endpoint and a Server in an IP telephony network. In the embodiments discussed herein, a cable telephony adapter (CTA) device is representative of the IP telephony endpoint and a Signaling Controller (SC) is representative of the Server. However, the present invention is suitable for use with other types of network endpoints and Servers not discussed herein.

FIG. 1 shows a portion of a telephony network **100** constructed in accordance with the present invention. To access the telephony network, CTA **102** provides access to a user **104** via a Hybrid Fiber/Coax (HFC) head-end **106**. The HFC head-end **106** has the capacity to provide access to other users as shown at **108**. The HFC head-end is also coupled to a Signaling Controller (SC) **110** which is coupled to a telephony network backbone **114**. The Signaling Controller is used to control the CTA's access to the telephony network. A key distribution center (KDC) **112**, is also coupled to the telephony network backbone **114**. The KDC **112** issues Kerberos tickets, which are in turn used to generate sub-keys for secure connection protocols, such as the IPSec encapsulating security payload (ESP) protocol, or other secure connections. The network **100** also includes a customer service representative (CSR) center **116**, a provisioning certification authority (CA) **118** and a billing host **120**.

Thus, in the network **100** it is possible for the user **104** to access the telephony backbone **114** via the CTA **102** using a secure protocol.

Embodiments of the present invention include the use of the Kerberos protocol with the public key PKINIT extension for key management. This protocol is based on Kerberos tickets, which may becookies, encrypted with the particular server's key. The Kerberos ticket is used to both authenticate a client to a server and to establish a session key, which is contained in the ticket. Accessing Kerberos services can be done using the Generic Security Service Application Program Interface (GSS-API) standard.

In one embodiment of the present invention, two-way authentication with public key certificates is used by the CTA to obtain a security ticket in the form of a Signaling Controller ticket from the KDC. A corresponding session key is delivered to the CTA sealed with either the CTA's public key or with a secret derived from a Diffie-Hellman exchange. The Signaling Controller ticket is kept for a relatively long period of time, for example, days or weeks. The length of this period can be adjusted based on network performance requirements. In addition, the Signaling Controller ticket is used to establish a symmetric session key, which is in turn used to establish a set of keys for use with the IPSec ESP mode. The keys used by IPSec are not derived from the session key itself. Instead, another random key (i.e., a sub-key) is generated for each phone call and then used to derive the IPSec keys. Thus, the Signaling Controller does not have to keep state. After it derives all the required keys from the sub-key and exchanges signaling messages with the CTA, the Signaling Controller can throw away the ticket along with all of the associated keys.

The use of the Kerberos protocol with the PKINIT extension in embodiments of the present invention provides several advantages. For example, the Signaling Controller is not required to keep state - Kerberos tickets need to be kept only by the endpoints (CTAs). Also, **IPSec** Security Associations can be torn down when no longer needed and quickly re-established with efficient key management based on the Kerberos tickets. The protocol runs over both TCP and UDP protocols, and is a widely available standard, with multiple vendors providing support for both Kerberos and PKINIT.

In one embodiment, within the PKINIT protocol, RSA is used for both key delivery and authentication. In another embodiment a PKINIT option may be used wherein Diffie-Hellman is used for the key exchange and RSA is used for authentication. In general, embodiments of the present invention are suitable for use with any public key algorithms within PKINIT for both authentication and key exchanges.

FIG. **2** shows a message exchange diagram **200** illustrating how the CTA uses Kerberos to obtain the sub-key, which in turn, is used to derive IPSec ESP keys for the CTA-to-Signaling Controller signaling messages. In the exchange diagram **200**, only some of the information carried in the messages is provided in order to present a clear description of the protocol. The exchange diagram **200** shows messages transmitted or received at the CTA **102** at line **220**, the KDC **112** at line **222**, and the Signaling Controller **110** at line **224**.

FIG. **3** shows a flow diagram **300** illustrating how the messages of FIG. **2** are exchanged in accordance with the present invention.

At block **302**, a PKINIT Request requesting a security ticket, which could be of the form of the Kerberos ticket detailed above, is sent from the CTA **102** to the KDC **112** as shown by message **202**. This request includes the CTA signature and certificate - used by the KDC to authenticate the CTA. This request also carries the current time - used by the KDC to verify that this message is not a replay or a retransmission of an old message. The PKINIT Request also contains a random value (called a nonce) that will be used to bind a subsequent PKINIT Reply message to this request. In the case that a Diffie-Hellman exchange is used, the CTA will also include its Diffie-Hellman parameters and public value in the PKINIT Request.

At block **304**, the KDC **112** receives and verifies the PKINIT Request and then issues to the CTA a security ticket for the Signaling Controller (also referred to as a Signalling Controller ticket) encrypted with the Signaling Controller's service key. Inside this encrypted ticket are a symmetric session key, its validity period and the CTA identity. Also in this step, this ticket will be sent back to the CTA **102** inside a PKINIT Reply, shown by message **204**. The PKINIT Reply message also contains KDC's certificate and signature for authenticating the KDC, along with the nonce

from the PKINIT Request to protect against replays. If a Diffie-Hellman exchange is used, the KDC also places its Diffie-Hellman public value into this message.

The PKINIT Reply also contains a second copy of the session key and its validity period found in the ticket - intended to be decrypted and used by the CTA. This second copy of the session key and its associated attributes are either encrypted with a Diffie-Hellman-derived secret or enveloped with the CTA's public key. Here, enveloped means that the session key along with its associated attributes are not encrypted directly with the CTA's public key. Within the PKINIT Reply the public key is used to encrypt a random symmetric key that is in turn used to encrypt another symmetric key which is then finally used to encrypt the session key and its attributes. This embodiment uses the PKINIT standard as is, even though in this case, simplifications to the PKINIT Reply seem possible. If a Diffie-Hellman exchange is not used, then the Reply contains message items as shown at **226**.

At block **306**, an application (AP) Request requesting a sub-key is sent from the CTA **102** to the Signaling Controller **110** as shown by message **206**. Here, a CTA has already obtained a Signaling Controller ticket and now initiates key management with the Signaling Controller by sending it an AP Request message. The AP Request contains the Signaling Controller ticket along with the CTA name, timestamp and a message hash – all encrypted with the SC session key. The timestamp is used to check for replays of old AP Request messages.

At block **308**, the Signaling Controller **110** receives an AP Request. It first decrypts and validates the ticket with its service key. It then takes the session key out of the ticket and uses it to decrypt and validate the rest of the AP Request. Then, the Signaling Controller generates a random sub-key and encrypts it along with the current timestamp with the session key. It places this information into an AP Reply message **208** and sends it back to the CTA.

At block **310**, the CTA receives and validates the AP Reply, after which it shares the sub-key with the Signaling Controller. Both sides independently derive (with some one-way function) a set of IPSec encryption and authentication keys from this sub-key. After that, all signaling messages between the CTA and the Signaling Controller will be protected with an IPSec channel. This establishment of the IPSec

channel is symbolically illustrated in FIG. **2** at **210** - even though this step does not involve an exchange of messages.

In the embodiment of the invention depicted in FIGS. **2** and **3**, the PKINIT exchange is performed at long intervals in order to obtain an intermediate symmetric session key. This session key is shared between the CTA and the Signaling Controller (via the Signaling Controller Ticket).

In this embodiment, the PKINIT Request/Reply messages, shown at **202** and **204**, are sent over a TCP/IP connection. This is because a single PKINIT Request or Reply message, containing public key and Diffie-Hellman information may be too large to fit into a single UDP packet. The use of TCP instead of UDP may have some impact on performance, but since the PKINIT exchange occurs at infrequent intervals (days or weeks apart) and is not tied to the phone calls, the impact on performance is not significant.

The session key is used in the AP Request and AP Reply messages shown at **206,208,** which are exchanged for each phone call, to establish a symmetric sub-key. This sub-key is used to derive all of the IPSec ESP keys and starting sequence numbers, used for both directions. The AP Request and AP Reply messages are small enough to fit into a single UDP packet, and thus will run over UDP.

The present invention provides a highly scalable key management architecture for secure client-server systems used in IP telephony networks. It will be apparent to those with skill in the art that modifications to the above methods and embodiments can occur without deviating from the scope of the present invention. Accordingly, the disclosures and descriptions herein are intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A secure IP telephony system, the system comprising:

a signaling controller within an IP telephony network and in communication with at least one Cable Telephony Adapter (CTA), and configured to generate a symmetric sub-key in response to a request from the at least one CTA, the request including a signaling controller ticket;

wherein the signaling controller ticket comprises a signaling controller session key, an identity of the at least one CTA, and an identity of the signaling controller;

the signaling controller further configured to distribute the symmetric sub-key to the at least one CTA in response to the signaling controller ticket; and

a Key Distribution Center (KDC) within the IP telephony network and coupled to the signaling controller, and configured to generate and distribute the signaling controller ticket and said signaling controller session key to the at least one CTA using public key encryption,

wherein said at least one CTA generates an additional symmetric key specific for a given call based on the symmetric sub-key provided by the signaling controller that is utilized for the given call for CTA to CTA signaling or bearer channel communication.

2. The system of claim 1, wherein the signaling controller is configured to generate and distribute the symmetric sub-key in response to a Kerberos request from the at least one CTA.

3. The system of claim **1**, wherein the signaling controller distributes the sub-key encrypted with the signaling controller session key.

4. The system of claim **1**, wherein the signaling controller receives from the at least one CTA the signaling controller ticket, wherein a portion of the signaling controller ticket is encrypted with a signaling controller server key.

5. The system of claim **1**, wherein the request comprises a Kerberos Application Request having the signaling controller ticket and encrypted data including a name of the at least one CTA.

6. The system of claim **1**, wherein the request includes a timestamp.

7. The system of claim **1**, wherein the signaling controller authenticates the at least one CTA using the signaling controller ticket.

8. The system of claim **1**, wherein the signaling controller communicates with the CTA in an IPsec ESP session in response to receiving a valid signaling controller ticket.

9. The system of claim **1**, wherein the KDC generates and distributes the signaling controller ticket in a Kerberos exchange with the at least one CTA.

10. The system of claim **9**, further comprising a Provisioning Certificate Authority (CA) in communication with the IP telephony network configured to receive a manufacturer signed CTA certificate and distribute an operator network-specific certificate to the at least one CTA.

11. The system of claim **1**, wherein the signaling controller ticket comprises a Kerberos ticket.

12. The system of claim **1**, wherein the signaling controller ticket further comprises an expiration time.

13. The system of claim **1**, wherein the KDC distributes to the at least one CTA the signaling controller ticket and a copy of the session key outside of the signaling controller ticket encrypted with a CTA public key.

14. The system of claim **1**, wherein the KDC distributes the signaling controller ticket to the at least one CTA, and also distributes to the at least one CTA a copy of the session key outside of the signaling controller ticket encrypted using a shared secret derived from a Diffie-Hellman exchange.

15. The system of claim **1**, wherein said additional symmetric key is valid for a single call.

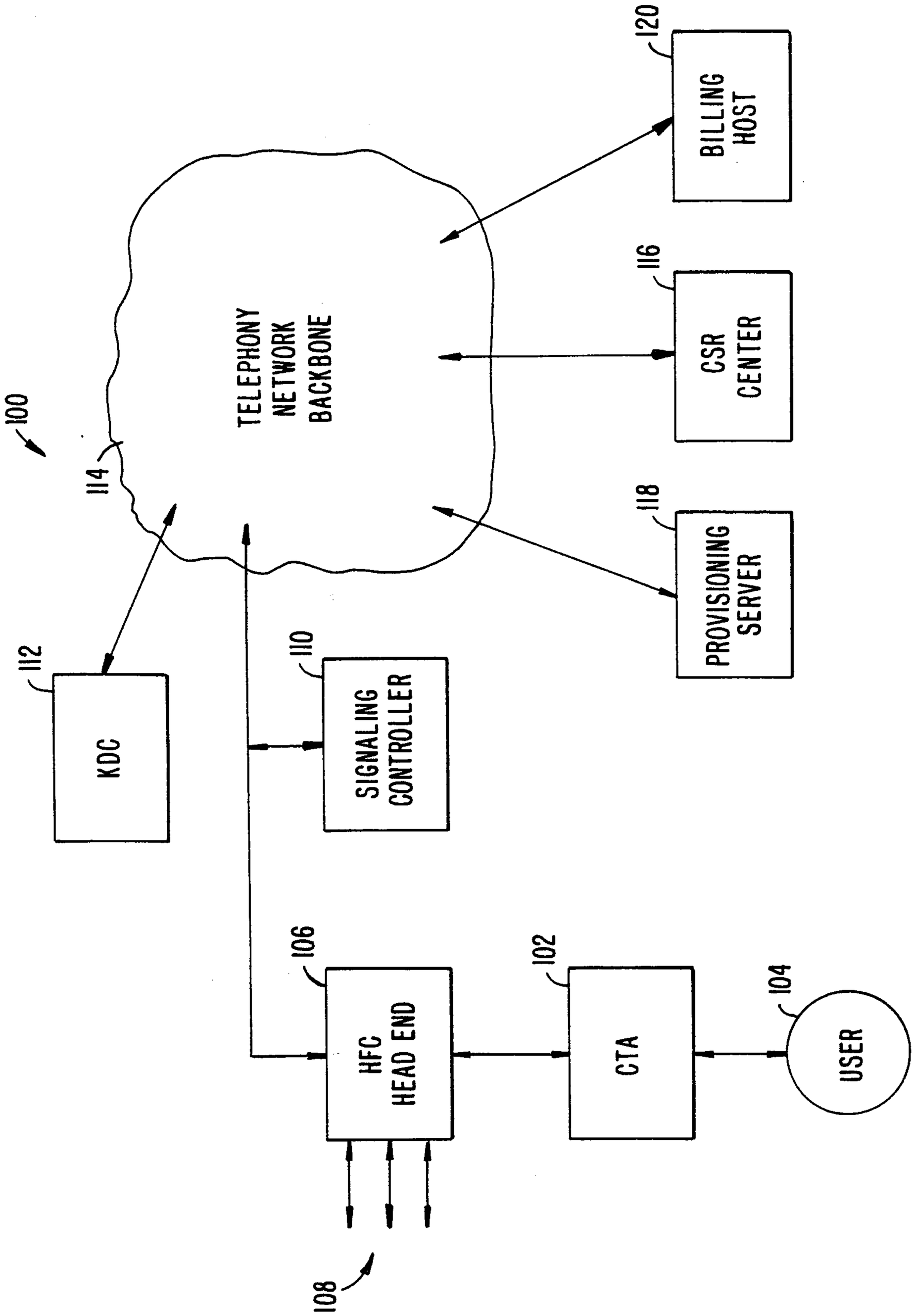

100
112
KDC
114
TELEPHONY NETWORK BACKBONE
120
BILLING HOST
116
CSR CENTER
118
PROVISIONING SERVER
110
SIGNALING CONTROLLER
106
HFC HEAD END
102
CTA
104
USER
108

FIG. 1.

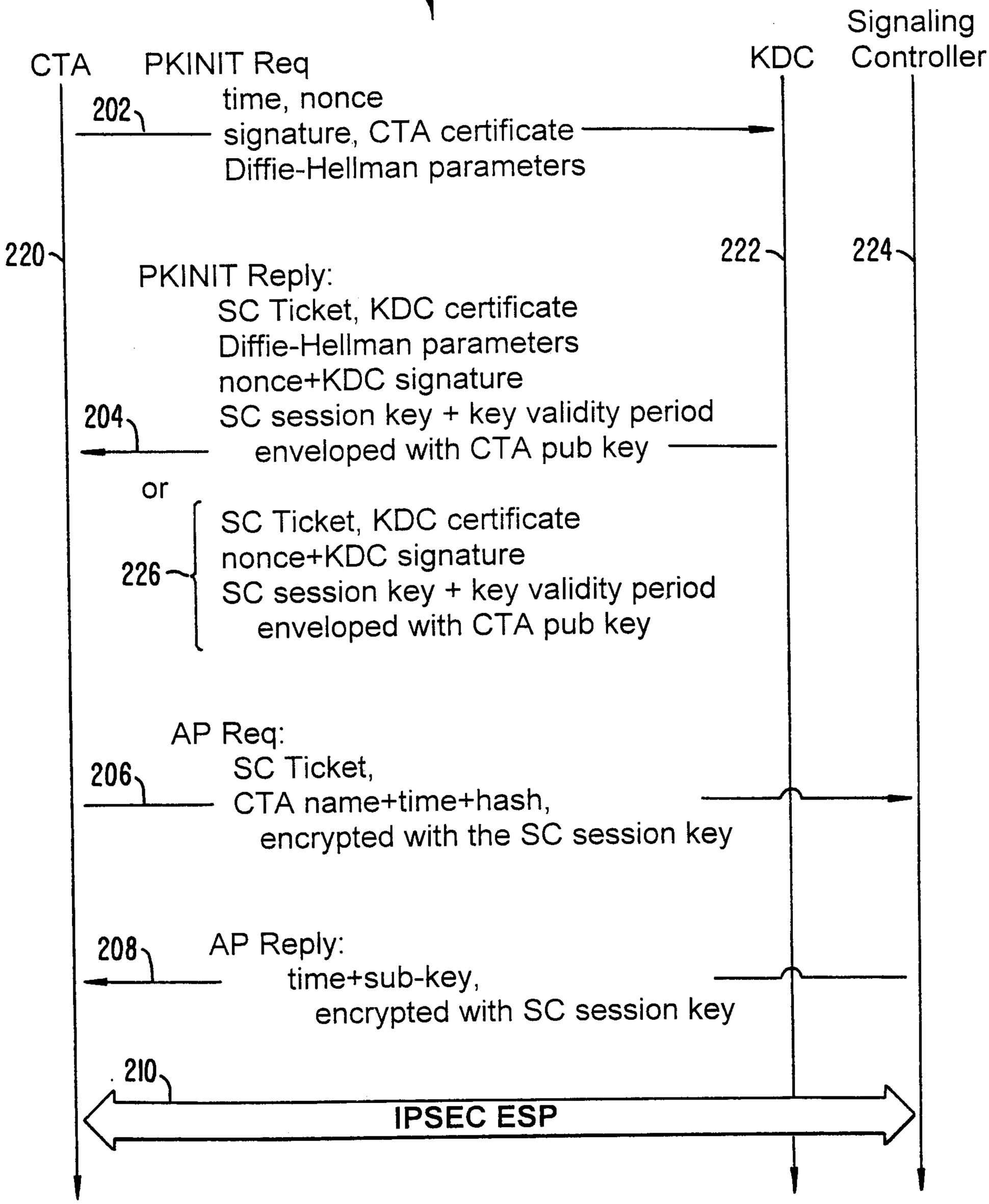

200
CTA
PKINIT Req
time, nonce
202
signature, CTA certificate
Diffie-Hellman parameters
KDC
Signaling Controller
220
222
224
PKINIT Reply:
SC Ticket, KDC certificate
Diffie-Hellman parameters
nonce+KDC signature
204
SC session key + key validity period
enveloped with CTA pub key
or
226
SC Ticket, KDC certificate
nonce+KDC signature
SC session key + key validity period
enveloped with CTA pub key
AP Req:
206
SC Ticket,
CTA name+time+hash,
encrypted with the SC session key
208
AP Reply:
time+sub-key,
encrypted with SC session key
210
IPSEC ESP

FIG. 2.

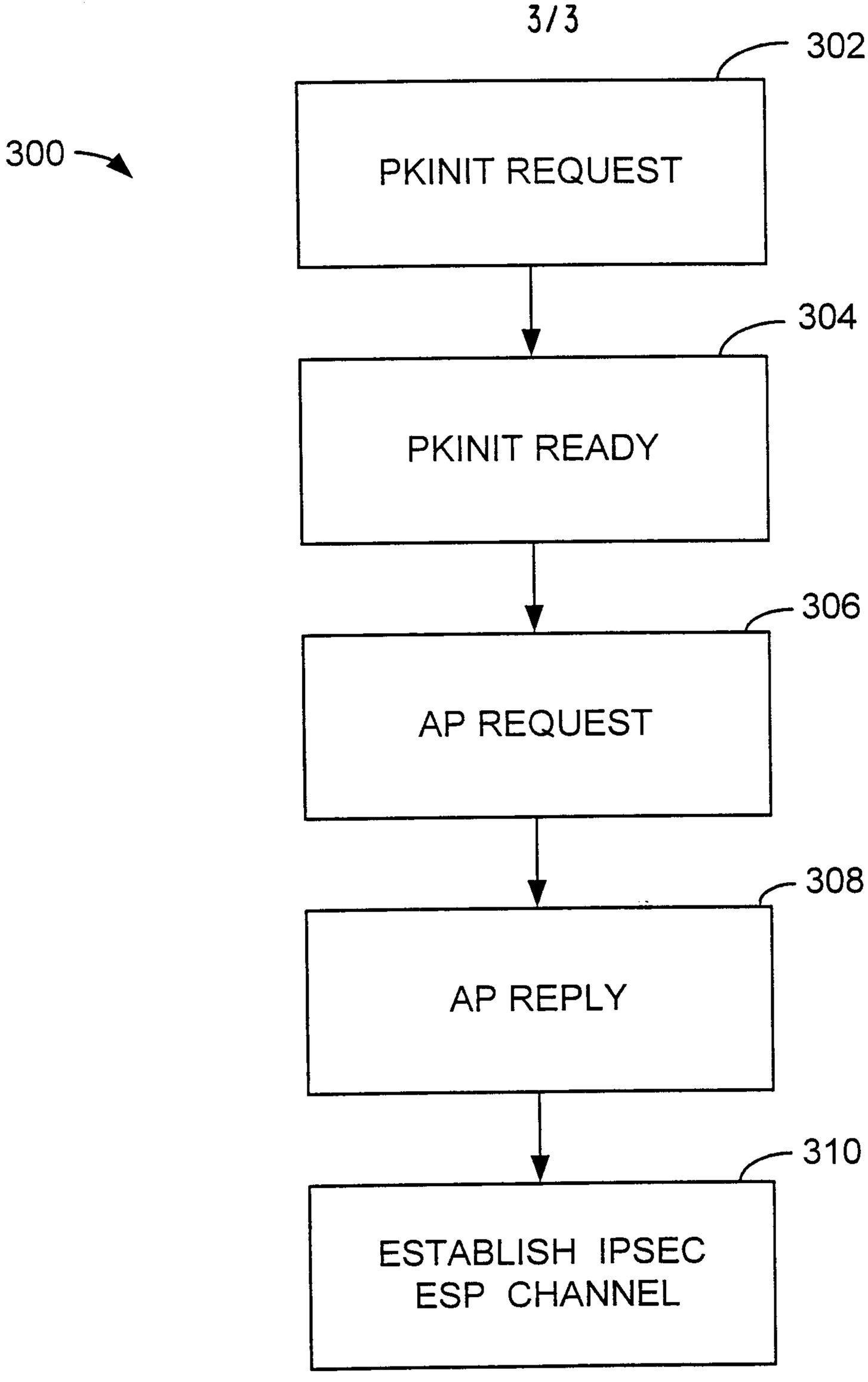
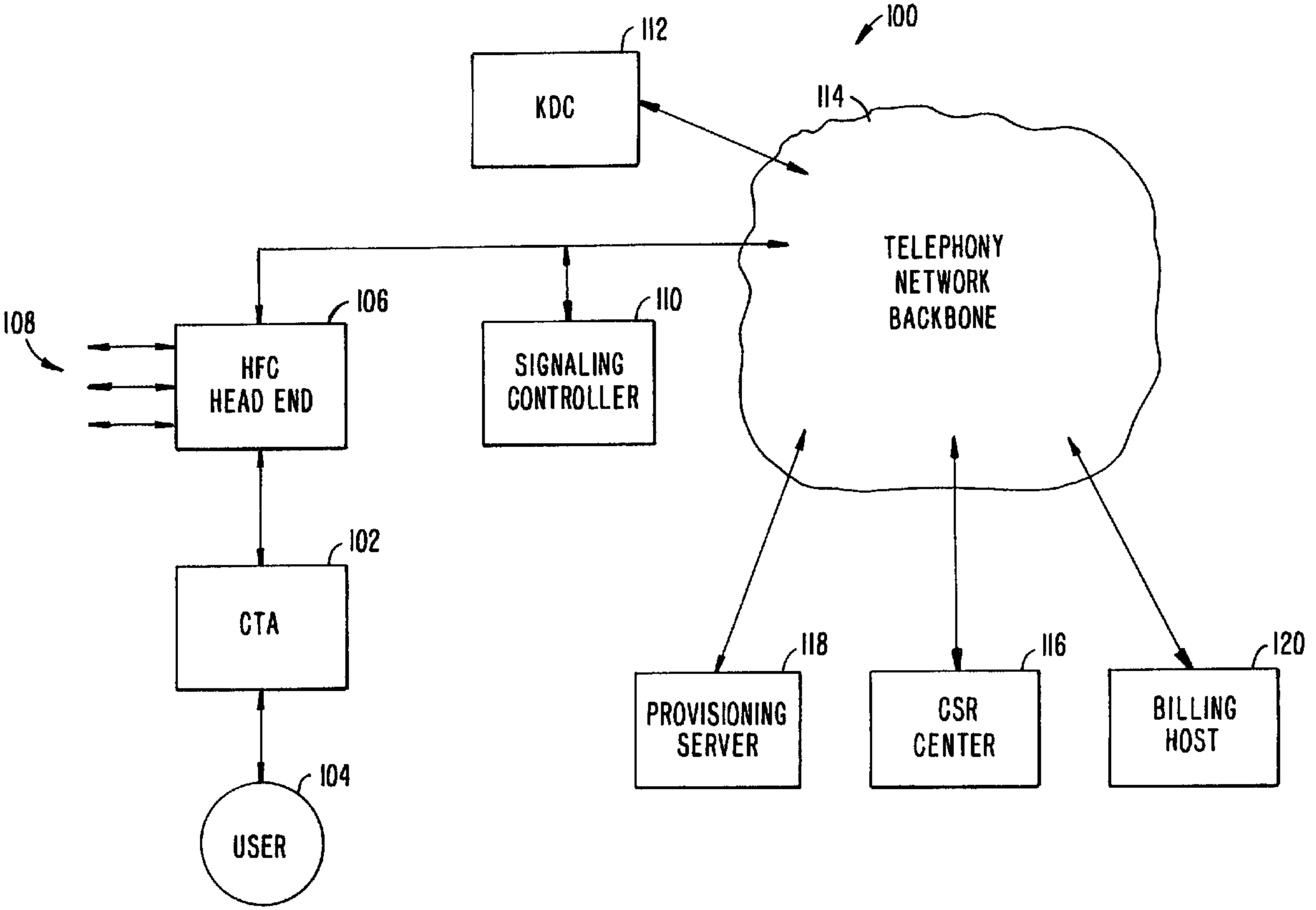

300
302
PKINIT REQUEST
304
PKINIT READY
306
AP REQUEST
308
AP REPLY
310
ESTABLISH IPSEC
ESP CHANNEL

FIG. 3.


100
112
KDC
114
TELEPHONY
NETWORK
BACKBONE
108
106
HFC
HEAD END
110
SIGNALING
CONTROLLER
102
CTA
104
USER
118
PROVISIONING
SERVER
116
CSR
CENTER
120
BILLING
HOST