(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 April 2006 (27.04.2006)

PCT

(10) International Publication Number
WO 2006/045014 A2

(51) International Patent Classification:
H04N 7/167 (2006.01)

(21) International Application Number:
PCT/US2005/037732

(22) International Filing Date: 20 October 2005 (20.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/620,495	20 October 2004 (20.10.2004)	US
11/253,346	19 October 2005 (19.10.2005)	US

(71) Applicant and
(72) Inventor: **MARKEY, John, Kevin** [US/US]; 12436 Kestrel Street, San Diego, CA 92129 (US).

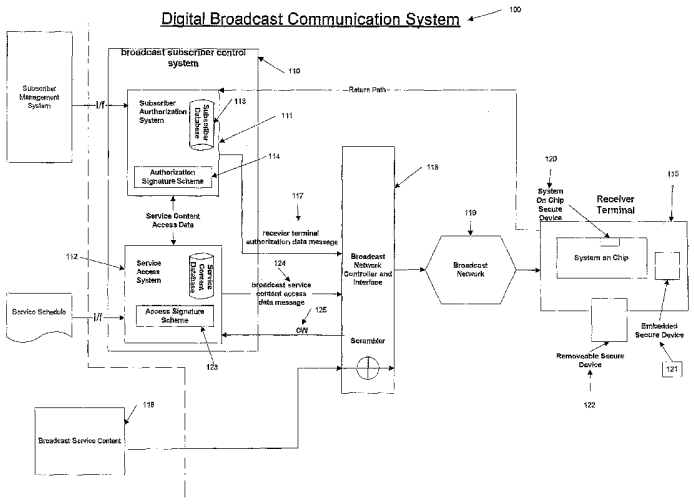
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** APPLICATION OF ASYMMETRIC DIGITAL SIGNATURE SCHEME TO BROADCAST SYSTEM



(57) **Abstract:** Methods and devices that implement asymmetric cryptographic system based digital signatures to the management of message tampering and assurance of message integrity in an access control system of digital broadcast services. In one embodiment, the receiver terminal authorization data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a broadcast private-public digital signature scheme key pair. The receiver terminals of the broadcast network receive these authorization data messages. The digital signature of each authorization data message is tested for authenticity with the public key of the broadcast subscriber control system. In a second embodiment, the receiver terminal authorization data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a plurality of private-public key pairs, with unique digital signature private-public key pairs, one for each receiver terminal. The receiver terminals of the broadcast network receive these authorization data messages. The digital signature of each authorization data message is tested for authenticity with the specific public key of the private-public key pair associated with the specific receiver terminal. Authorization data messages are only determined to be valid and subsequently utilized in the receiver terminal to modify the authorizations or deliver necessary data of the receiver terminal if the digital signature is valid. In both embodiments, the broadcast service content access data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a private key unique to the broadcast access control system. The receiver terminals of the broadcast network receive these broadcast service content access data messages. The digital signature of each message is tested for authenticity with the public key of the broadcast subscriber control system. Broadcast service content access data messages are utilized to control access to the broadcast services by the receiver terminal if the digital signature is authentic.

WO 2006/045014 A2

TITLE OF THE INVENTION

APPLICATION OF ASYMMETRIC DIGITAL SIGNATURE SCHEME TO BROADCAST SYSTEM

Priority is claimed based on provisional application number 60/620,495.

BACKGROUND OF THE INVENTION

Field of the Invention

The invention relates to the use of asymmetric digital cryptographic signature schemes for secure communications in a broadcast network.

Discussion of the Background

Broadcast subscriber control systems used for controlling access in the broadcasting of information to users which are known to the broadcaster, where the broadcaster wishes to make unauthorized, unknown access to the broadcast difficult, have been deployed for many decades. In the '70's and '80's these systems began to use cryptographic methods to help to control access with limited success. Piracy has plagued all of the systems that have been used until today including systems deployed for satellite, cable and terrestrial (UHF, VHF) broadcasts. Here we describe a system utilizing additional, as yet not used in these systems, cryptographic (Asymmetric Digital Signature Scheme) methods that have the purpose of ensuring the security robustness of these systems.

Broadcast subscriber control systems utilize two types of data messages that are broadcast throughout the network that are received by receiver terminals for the purpose of access control:

- Receiver terminal authorization data message,
- Broadcast service content access data message.

Both of these critical messages for the control of access to the broadcast services have been the points of attack for unauthorized access.

Receiver terminal authorization data messages have been counterfeited and authorizations not originating from the broadcast subscriber control system have been an attack on the control of access. A common problem with existing systems has been the use of symmetric cryptography based MAC (Message Authentication Code) of the receiver terminal authorization data message, that is generated in the broadcast subscriber control system utilizing a symmetric cipher scheme: Problem, once an authorized and authentic receiver terminal is reverse engineered then all keys and necessary methods used to create the MAC of the receiver terminal authorization data message can be accessed then counterfeit messages can be created. Thus, counterfeit authorizations can be sent to any receiver terminal.

In current systems a broadcast service content access data message can suffer a direct attack on access control to broadcast content because often this attack results in access to the information necessary to successfully receive the content. Attack directly on the broadcast service content access data message robustness occurs when the symmetric cryptographic MAC used to sign the broadcast service content access data message, utilized in order to maintain a test of its integrity uses either a symmetric key or a one-way hash, keyed or fixed key. This has very often led to pirate attack by modification of the contents of the broadcast service content access data message and generation of a counterfeit broadcast service content access data message with modified contents, the keys and necessary methods are known to the counterfeiter from a source of valid keys and methods, such as from the reverse engineering of any authentic receiver terminal.

The use of asymmetric cryptographic system based digital signature scheme to the management of message tampering and assurance of message integrity in an access control system of digital broadcast services:

Asymmetric digital signature of broadcast service content access data messages: All broadcast service content access data messages are digitally signed with a private key utilizing an access digital signature scheme of the broadcast subscriber control system. This signature is tested for authenticity in the receiver terminal utilizing a corresponding access public key of the broadcast subscriber control system.

Asymmetric digital signature of receiver terminal authorization data messages: All receiver terminal authorization data messages are digitally signed with a private key utilizing an authorization digital signature scheme of the broadcast subscriber control system. This signature is tested for authenticity in the receiver terminal with a corresponding authorization public key of the broadcast subscriber control system. Alternately, all receiver terminal authorization data messages are digitally signed with a private key unique to each receiver terminal utilizing an authorization digital signature scheme of the broadcast subscriber control system. This signature is tested for authenticity in the receiver terminal with a corresponding authorization public key unique to each receiver terminal of the digital broadcast communication system.

SUMMARY OF THE INVENTION

The present invention provides methods and apparatus for the implementation of asymmetric cryptographic system based digital signatures to the management of message tampering and assurance of message integrity in an access control system of digital broadcast services. In one embodiment, the receiver terminal authorization data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a broadcast subscriber control system private-public digital signature scheme key pair. The receiver terminals of the broadcast network receive these authorization data messages. The digital signature of each authorization data

message is tested for authenticity with the public key of the broadcast subscriber control system. In a second embodiment, the receiver terminal authorization data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a plurality of private-public key pairs, with unique digital signature private-public key pairs, one for each receiver terminal. The receiver terminals of the broadcast network receive these authorization data messages. The digital signature of each authorization data message is tested for authenticity with the specific public key of the private-public key pair associated with the specific receiver terminal. Authorization data messages are only determined to be valid and subsequently utilized in the receiver terminal to modify the authorizations or deliver necessary data of the receiver terminal if the digital signature is valid. In both embodiments, the broadcast service content access data messages from the broadcast subscriber control system are digitally signed by a digital signature scheme utilizing a private key unique to the broadcast subscriber control system. The receiver terminals of the broadcast network receive these broadcast service content access data messages. The digital signature of each message is tested for authenticity with the public key of the broadcast subscriber control system. Broadcast service content access data messages are utilized to control access to the broadcast services by the receiver terminal only if the digital signature is authentic.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant features and advantages thereof will be readily obtained as the same become better

understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

Figure 1 is a logical block diagram of a digital broadcast communication system

Figure 2 is a logical block diagram of the authorization asymmetric digital signature scheme of the first preferred embodiment

Figure 3 is a logical block diagram of the authorization asymmetric digital signature scheme of the second preferred embodiment

Figure 4 is a logical block diagram of the access asymmetric digital signature scheme

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention will be discussed with reference to preferred embodiments of digital broadcast communication systems. Specific details, such as number of keys and types of messages, and references to standards, set forth in order to provide a thorough understanding of the present invention. The preferred embodiments discussed herein should not be understood to limit the invention. Furthermore, for ease of understanding, certain method steps are delineated as separate steps; however, these steps should not be construed as necessarily distinct nor order dependent in their performance.

The present invention is believed to be particularly applicable to the field of pay television and hence will be discussed primarily in that context. Those of skill in the art will recognize that the invention may be applied in many other settings and is not limited to pay television.

Referring now to the drawings, wherein like reference numerals designate

identical or corresponding parts throughout the several views, Figure 1 is a logical block diagram of a digital broadcast communication system 100. The system 100 comprises a broadcast subscriber control system 110. The broadcast subscriber control system of Figure 1 is comprised of two parts: subscriber authorization system 111 and service access system 112.

The subscriber authorization system 111 of Figure 1 is comprised of two parts: subscriber database 113 and authorization signature scheme 114. The subscriber authorization system 111 stores the subscriber database 113 of authorizations for each receiver terminal 115 that are the authorizations of each corresponding subscriber to the broadcast service content 116. Broadcast service content 116 can be television, radio, movie, as only examples of any possible broadcast service content 116. The subscriber authorization system 111 creates receiver terminal authorization data message 117 that is transmitted to the broadcast network controller and interface 118 order for it to be broadcast into the broadcast network 119.

The invention first embodiment the authorization signature scheme 114 of Figure 1 generates an asymmetric digital signature of the receiver terminal authorization data message 117 that is appended by the authorization signature scheme 114 to said same receiver terminal authorization data message 117. In this first embodiment the private key 126 of the authorization signature scheme in Figure 2 is unique to the subscriber authorization system 111, but it is the same private key 126 used for all receiver terminal authorization data message 117 that are digitally signed by the authorization signature scheme 114.

The invention first embodiment in Figure 2 the authorization asymmetric digital signature scheme (AS1) 127 comprises the method of generation of the authorization asymmetric digital signature (S1) 128 using

the private key 126 of the authorization signature scheme 114, appending of the authorization asymmetric digital signature (S1) 128 to the receiver terminal authorization data message 117, broadcast 129 of the receiver terminal authorization data message 117, reception of the receiver terminal authorization data message 117 by the receiver terminal 115, test of the authenticity of the authorization asymmetric digital signature (AST1) 130 utilizing the unique public key 131 of the subscriber authorization system 111 where such test is performed inside a secure device; system on chip secure device 120, embedded secure device 121, removable secure device 122, of the receiver terminal 115, utilization 132 of the receiver authorization data message 117 within said secure device; system on chip secure device 120, embedded secure device 121, removable secure device 122, of the receiver terminal 115 only if the authorization asymmetric digital signature 128 is tested as valid. In this first embodiment the receiver terminal authorization data message 117 is received by the receiver terminal that has the corresponding address in the address data field of the receiver terminal authorization data message 117 where said address can be of three or more types: a unique receiver terminal address, a unique receiver terminal group address, which is comprised of a group number and a group mask bit value, or a global receiver terminal address. In this first embodiment the authorization asymmetric digital signature scheme 127 can be the same scheme for all receiver address types, or can be a unique authorization asymmetric digital signature scheme 127 unique for each type of address of the receiver terminals.

The invention first embodiment in Figure 2 the receiver terminal authorization data message 117 contains several data fields but not limited to: the address field

(unique, group, global); access authorization rights; authorization time code; authorization asymmetric digital signature 128.

The invention second embodiment the authorization signature scheme 114 of Figure 1 generates an asymmetric digital signature of the receiver terminal authorization data message 117 that is appended by the authorization signature scheme 114 to said same receiver terminal authorization data message 117. In this second embodiment the private key 133 of the authorization signature scheme 114 is unique to corresponding receiver terminal 115.

The invention second embodiment in Figure 3 the authorization asymmetric digital signature scheme 134 comprises the method of generation of the authorization asymmetric digital signature 135, appending of the authorization asymmetric digital signature to the receiver terminal authorization data message 117, broadcast 136 of the receiver terminal authorization data message 117, reception of the receiver terminal authorization data message 117 by the receiver terminal 115, test of the authenticity of the authorization asymmetric digital signature (AST2) 137 utilizing the unique public key 138 of the unique private-public key pair of the authorization asymmetric digital signature scheme 134 for the unique receiver terminal 115 where such test is performed inside a secure device; system on chip secure device 120, embedded secure device 121, removable secure device 122, of the receiver terminal 115, utilization 139 of the receiver terminal authorization data message 117 within said secure device; system on chip secure device 120, embedded secure device 121, removable secure device 122, of the receiver terminal 115 only if the authorization asymmetric digital signature is tested as valid. In this second embodiment the receiver terminal authorization data message 117 is received by the receiver terminal that has the corresponding address in the address data field of the receiver terminal authorization data message 117 where said address can be of three or more types: a unique receiver terminal address, a unique receiver

terminal group address, which is comprised of a group number and a group mask bit value, or a global receiver terminal address. In this second embodiment the authorization asymmetric digital signature scheme 134 can be the same scheme for all receiver address types, or can be a unique authorization asymmetric digital signature scheme 134 unique for each type of address of the receiver terminal.

The invention second embodiment in Figure 3 the receiver terminal authorization data message 117 contains several data fields but not limited to: the address field (unique, group, global); access authorization rights; authorization time code; authorization asymmetric digital signature 135.

The invention first and second embodiment the access signature scheme 123 of Figure 1 generates an asymmetric digital signature of the broadcast service content access data message 124 that is appended by the access signature scheme 123 to said same broadcast service content access data message 124. In the first and second embodiment of Figure 4 the private key 140 of the access signature scheme 123 is unique to the service access system 112, it is the same private key used for all broadcast service content access data message 124 that are digitally signed by access signature scheme 123.

The invention first and second embodiment in Figure 4 the access asymmetric digital signature scheme (ADS) 141 comprises the method of generation of access asymmetric digital signature 142, appending of the access asymmetric digital signature 142 to the broadcast service content access data message 124, broadcast 143 of the broadcast service content access data message 124, reception of the broadcast service content access data message 124 by the receiver terminal 115, test of the authenticity ADST 144 of the access asymmetric digital signature 142 utilizing the unique public key 145 of the service access system 112 where such test is performed inside a secure device; system on chip secure device 120, embedded secure device 121,

removable secure device 122, of the receiver terminal 115, utilization 146 of the broadcast service content access data message within said secure device; system on chip secure device 120, embedded secure device 121, removable secure device 122, of the receiver terminal 115 only if the access asymmetric digital signature 142 is tested as valid.

The invention first and second embodiment in Figure 4 the broadcast service content access data message 124 contains several data fields and not limited to: the transport service content encryption control word (CW) 125, access criteria, time code, access asymmetric digital signature 142.

Obviously, numerous other modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

WHAT IS CLAIMED IS:

1. A method for the delivery and control of access to broadcast signals, the method comprising the steps of:

generating a plurality of receiver terminal authorization data messages;

generating an asymmetric digital signature according to an authorization signature scheme of each receiver terminal authorization data message and appending said signature to each receiver terminal authorization data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of receiver terminal authorization data messages with authorization asymmetric digital signature appended to each receiver terminal authorization data message;

generating a plurality of broadcast service content access data messages;

generating an asymmetric digital signature of each broadcast service content access data message according to an access signature scheme and appending said signature to each broadcast service content access data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of broadcast service content access data messages with access asymmetric digital signature appended to each broadcast service content access data message;

receiving said receiver terminal authorization data message in a specific receiver terminal of corresponding address to the receiver terminal authorization data message;

testing the appended authorization asymmetric digital signature of said receiver terminal authorization data message in a secure device of the receiver terminal of the digital broadcast network according to the authorization asymmetric digital signature scheme and utilize the contents of said receiver terminal authorization data message

in said receiver terminal of the digital broadcast network only if the authorization asymmetric digital signature is valid ;

receiving said broadcast service content access data message necessary for access to broadcast service content;

testing the appended access asymmetric digital signature of said broadcast service content access data message in a secure device of the receiver terminal of the digital broadcast network according to the access asymmetric digital signature scheme and utilize the contents of said broadcast service content access data message in said receiver terminal of the digital broadcast network only if said asymmetric digital signature is valid.

2. The method of Claim 1, wherein the authorization asymmetric digital signature scheme is an asymmetric digital signature scheme comprising elliptic curve on finite field.

3. The method of Claim 1, wherein the access asymmetric digital signature scheme is an asymmetric digital signature scheme comprising elliptic curve on finite field.

4. The method of Claim 1, wherein the test of the authorization asymmetric digital signature and the utilize of the receiver terminal authorization data message is implemented in a SOC secure device.

5. The method of Claim 1, wherein the test of the authorization asymmetric digital signature and the utilize of the receiver terminal authorization data message is implemented in an embedded secure device.

6. The method of Claim 1, wherein the test of the authorization asymmetric digital signature and the utilize of the receiver terminal authorization data message is implemented in a removable secure device.

7. A method for the delivery and control of access to broadcast signals, the method comprising the steps of:

generating a plurality of receiver terminal authorization data messages;

generating an asymmetric digital signature according to an authorization signature scheme of each receiver terminal authorization data message and appending said signature to each receiver terminal authorization data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of receiver terminal authorization data messages with authorization asymmetric digital signature appended to each receiver terminal authorization data message;

receiving said receiver terminal authorization data message in a specific receiver terminal of corresponding address to the receiver terminal authorization data message;

testing the appended authorization asymmetric digital signature of said receiver terminal authorization data message in a secure device of the receiver terminal of the digital broadcast network according to the authorization asymmetric digital signature scheme and utilize the contents of said receiver terminal authorization data message in said receiver terminal of the digital broadcast network only if the authorization asymmetric digital signature is valid ;

8. The method of Claim 7, wherein the authorization asymmetric digital signature scheme is an asymmetric digital signature scheme comprising elliptic curve on finite field.

9. The method of Claim 7, wherein the test of the authorization asymmetric digital signature and the utilize of the receiver terminal authorization data message is implemented in an embedded secure device.

10. The method of Claim 7, wherein the test of the authorization asymmetric digital signature and the utilize of the receiver terminal authorization data message is implemented in a removable secure device.

11.The method of Claim 7, further comprising the step:

generating a plurality of broadcast service content access data messages;

generating an asymmetric digital signature of each broadcast service content access data message according to an access signature scheme and appending said signature to each broadcast service content access data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of broadcast service content access data messages with access asymmetric digital signature appended to each broadcast service content access data message;

receiving said broadcast service content access data message necessary for access to broadcast service content;

testing the appended access asymmetric digital signature of said broadcast service content access data message in a secure device of the receiver terminal of the digital broadcast network according to the access asymmetric digital signature scheme and utilize the contents of said broadcast service content access data message in said receiver terminal of the digital broadcast network only if said asymmetric digital signature is valid.

12. The method of Claim 11, wherein the access asymmetric digital signature scheme is an asymmetric digital signature scheme comprising elliptic curve on finite field.

13. The method of Claim 11, wherein the test of the access asymmetric digital signature and the utilize of the broadcast service content access data message is implemented in an embedded secure device.

14. The method of Claim 11, wherein the test of the access asymmetric digital signature and the utilize of the broadcast service content access data message is implemented in a removable secure device.

15. A method for the delivery and control of access to broadcast signals, the method comprising the steps of:

generating a plurality of broadcast service content access data messages;

generating an asymmetric digital signature of each broadcast service content access data message according to an access signature scheme and appending said signature to each broadcast service content access data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of broadcast service content access data messages with access asymmetric digital signature appended to each broadcast service content access data message;

receiving said broadcast service content access data message necessary for access to broadcast service content;

testing the appended access asymmetric digital signature of said broadcast service content access data message in a secure device of the receiver terminal of the digital broadcast network according to the access asymmetric digital signature scheme and utilize the contents of said broadcast service content access data message in said receiver terminal of the digital broadcast network only if said asymmetric digital signature is valid.

16. The method of Claim 15, wherein the access asymmetric digital signature scheme is an asymmetric digital signature scheme comprising elliptic curve on finite field.

17. The method of Claim 15, further comprising the step:

generating a plurality of receiver terminal authorization data messages;

generating an asymmetric digital signature according to an authorization signature scheme of each receiver terminal authorization data message and appending

said signature to each receiver terminal authorization data message before they are broadcast to the plurality of receiver terminals;

broadcasting to a plurality of receiver terminals a plurality of receiver terminal authorization data messages with authorization asymmetric digital signature appended to each receiver terminal authorization data message;

receiving said receiver terminal authorization data message in a specific receiver terminal of corresponding address to the receiver terminal authorization data message;

testing the appended authorization asymmetric digital signature of said receiver terminal authorization data message in a secure device of the receiver terminal of the digital broadcast network according to the authorization asymmetric digital signature scheme and utilize the contents of said receiver terminal authorization data message in said receiver terminal of the digital broadcast network only if the authorization asymmetric digital signature is valid ;

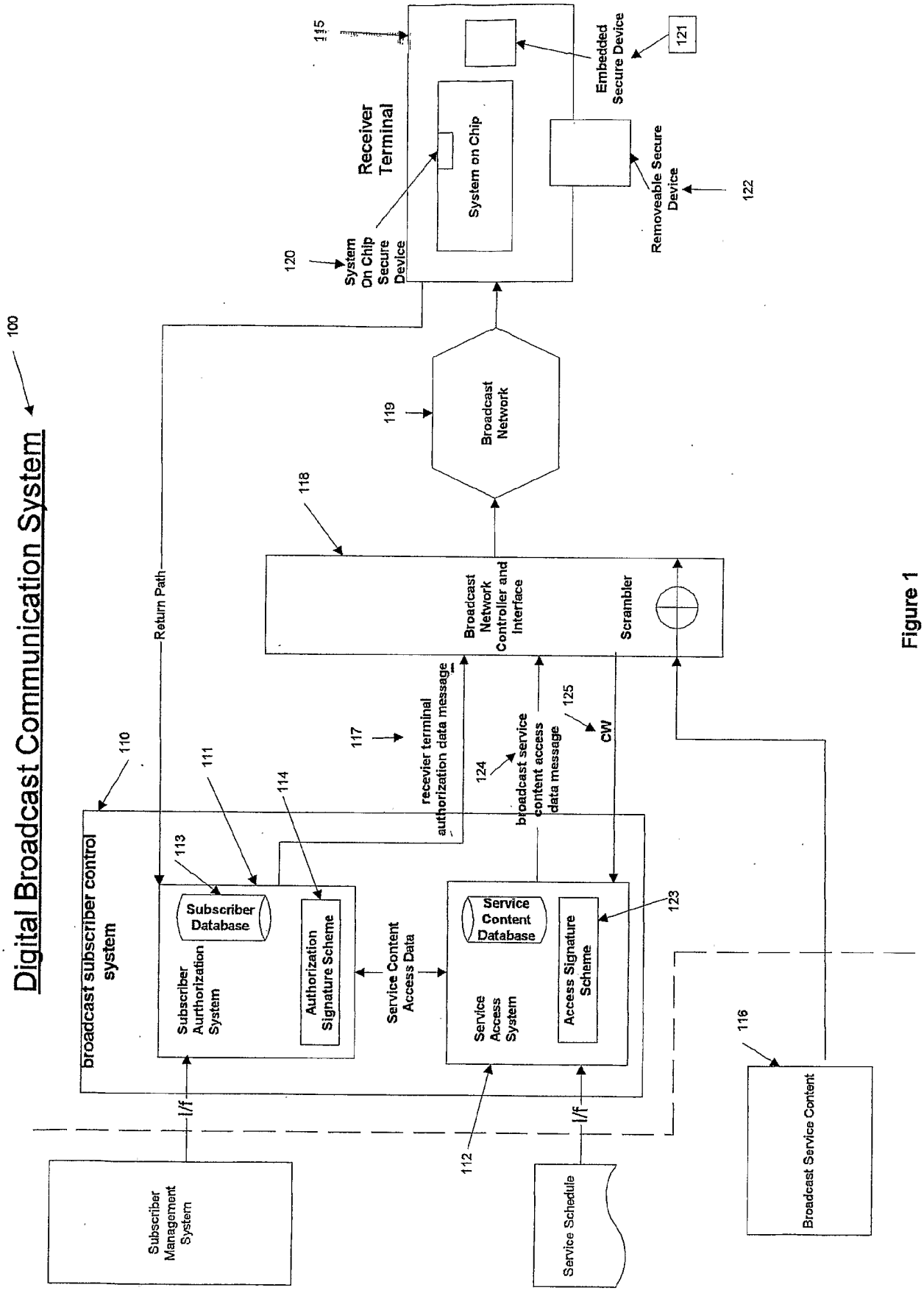

Digital Broadcast Communication System
100
Receiver Terminal
115
Embedded Secure Device
121
System on Chip
Removeable Secure Device
122
120
System On Chip Secure Device
119
Broadcast Network
118
Broadcast Network Controller and Interface
Scrambler
Return Path
recevier terminal authorization data message
117
broadcast service content access data message
124
CW
125
110
111
114
113
broadcast subscriber control system
Subscriber Database
Subscriber Aurthorization System
Authorization Signature Scheme
Service Content Access Data
Service Content Database
Service Access System
Access Signature Scheme
123
116
I/f
I/f
112
Subscriber Management System
Service Schedule
Broadcast Service Content

Figure 1

authorization asymmetric digital signature scheme of the first embodiment

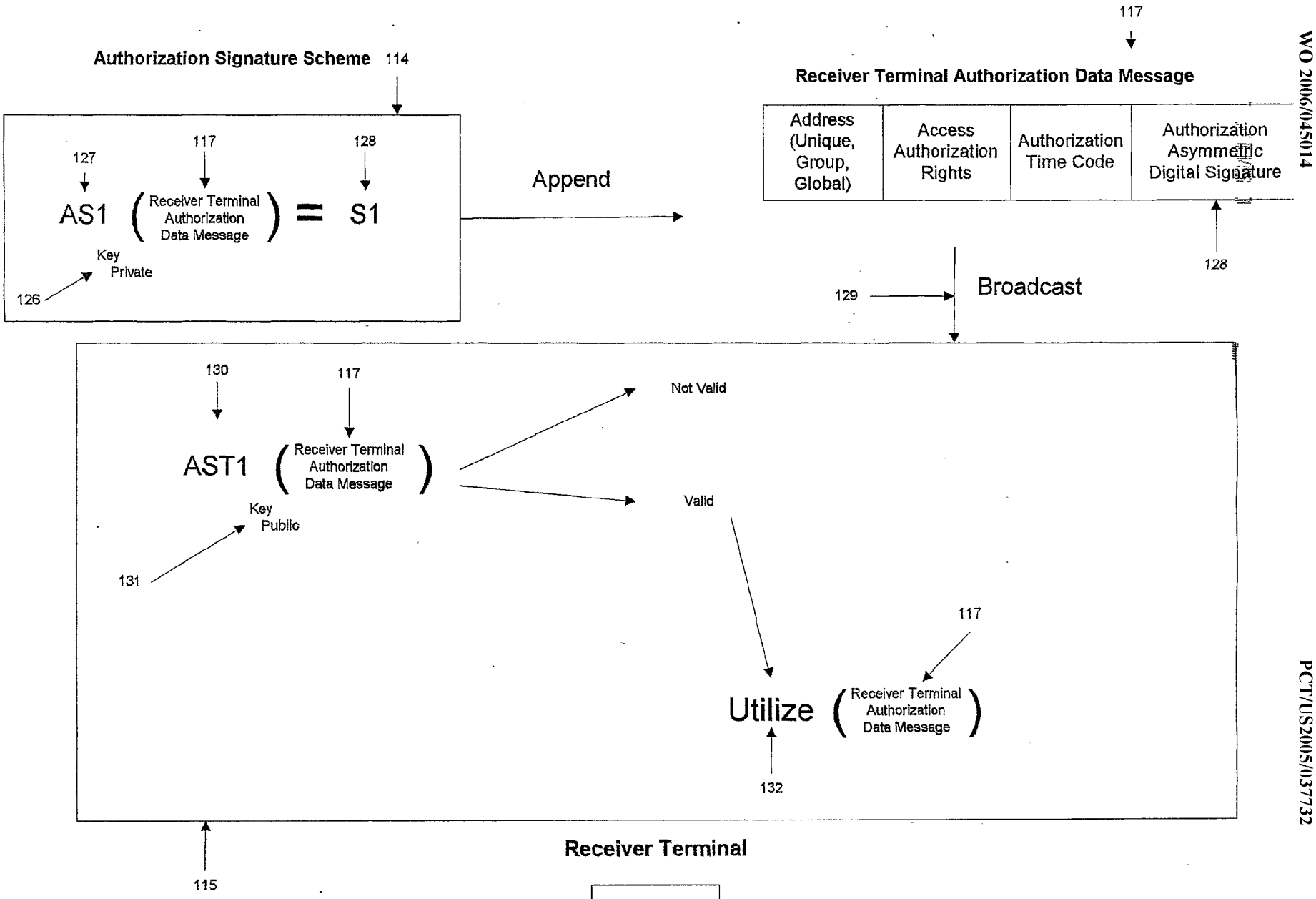


Figure 2

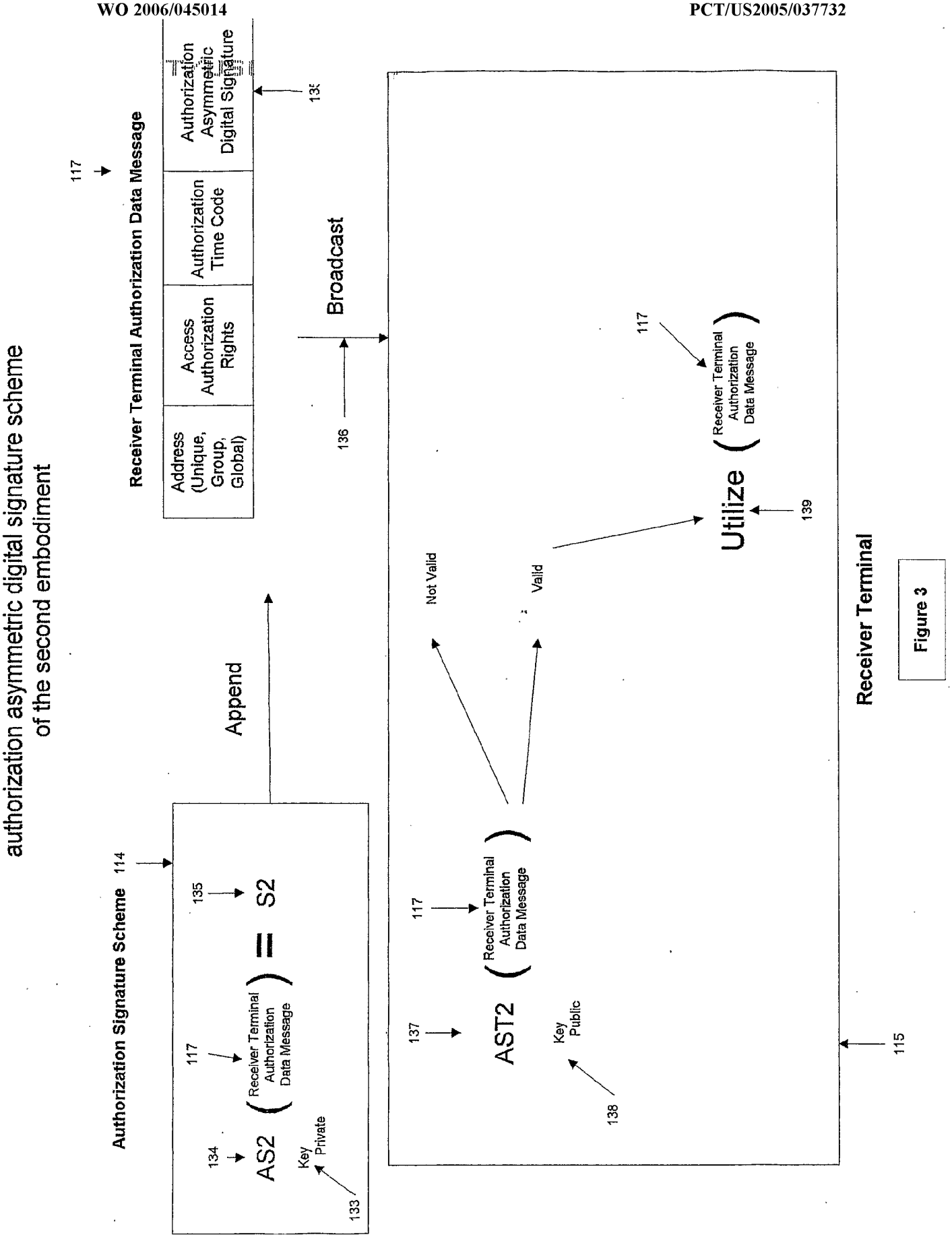

authorization asymmetric digital signature scheme
of the second embodiment
Authorization Signature Scheme 114
AS2 (Receiver Terminal Authorization Data Message) = S2
134
117
135
Key Private
133
Append
Receiver Terminal Authorization Data Message
117
Address (Unique, Group, Global)
Access Authorization Rights
Authorization Time Code
Authorization Asymmetric Digital Signature
136
Broadcast
Receiver Terminal
AST2 (Receiver Terminal Authorization Data Message)
137
117
Key Public
138
Not Valid
Valid
Utilize (Receiver Terminal Authorization Data Message)
139
117
115

Figure 3

access asymmetric digital signature scheme

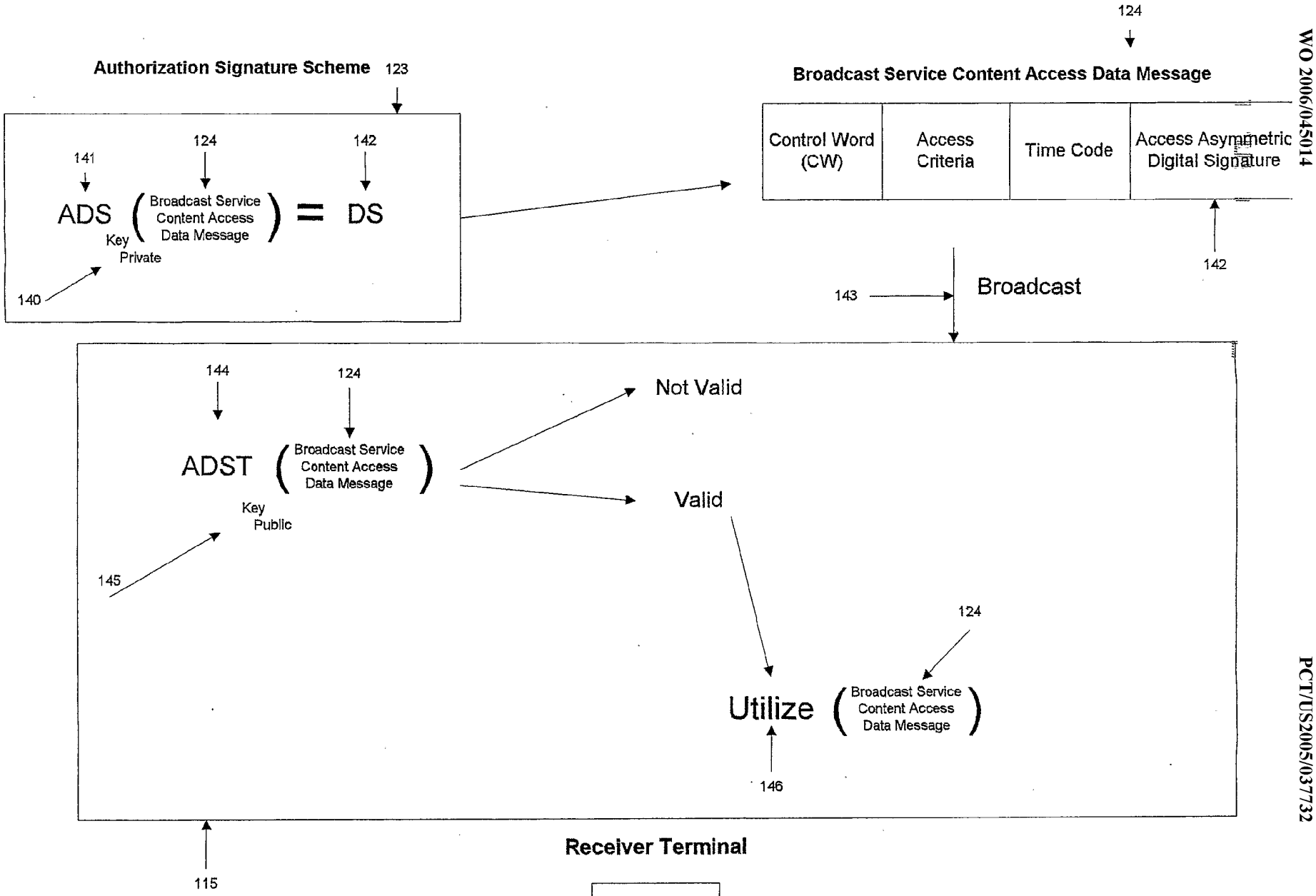


Figure 4