



(43) International Publication Date
23 August 2012 (23.08.2012)

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04W 12/06* (2009.01)
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/SG2012/000045

(22) International Filing Date:
14 February 2012 (14.02.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201101079-0 15 February 2011 (15.02.2011) SG
201105179-4 18 July 2011 (18.07.2011) SG
201108175-9 4 November 2011 (04.11.2011) SG

(71) Applicant (for all designated States except US):
**AGENCY FOR SCIENCE, TECHNOLOGY AND RE-
SEARCH** [SG/SG]; 1 Fusionopolis Way #20-10, Connex-
is, Singapore 138632 (SG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TEO, Chee Ming
Joseph** [SG/SG]; c/o PKM, Institute for Infocomm Re-
search, 1 Fusionopolis Way, #21-01 Connexis South
Tower, Singapore 138632 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**;
P.O. Box 1088, Rochor Post Office, Rochor Road, Singa-
pore 911833 (SG).

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

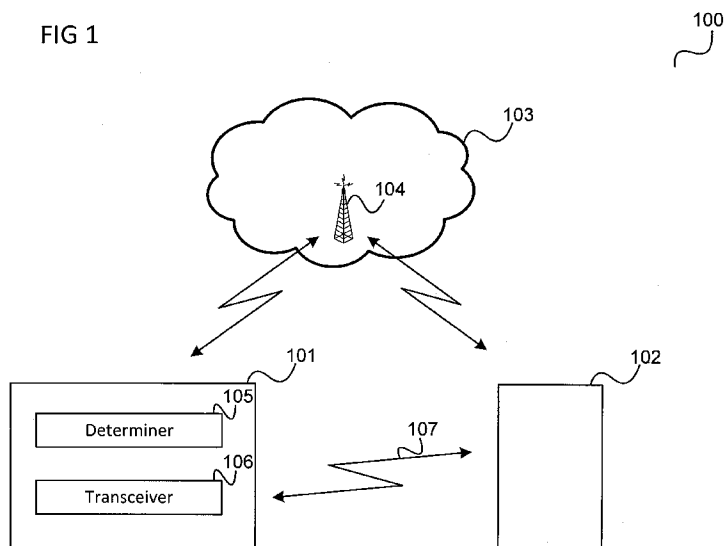
(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: COMMUNICATION TERMINAL AND METHOD FOR PERFORMING COMMUNICATION

FIG 1



(57) Abstract: A communication terminal of a cellular mobile communication system is described, the cellular mobile communication system comprising the communication terminal, another communication terminal and a communication network for providing a communication connection between the communication terminal and the other communication terminal via at least one base station of the communication network, the communication terminal comprising a determiner configured to determine an encryption key for secure communication between the communication terminal and the other communication terminal via a radio interface between the communication terminal and the other communication terminal; and a transceiver configured to perform secure communication with the other communication terminal via the radio interface between the communication terminal and the other communication terminal using the determined encryption key.

**COMMUNICATION TERMINAL AND METHOD FOR PERFORMING
COMMUNICATION**

5 Field of the invention

Embodiments of the invention generally relate to a communication terminal and a method for performing communication.

10

Background of the invention

The IEEE 802.16n System Requirements Document (SRD) specifies
15 a requirement for High Reliability (HR) network. As such, one
of the requirements is for the mobile stations (HR-MSs) to
communicate directly with each other in the event of network
failure. The HR-MS to HR-MS direct communications scenario
could for example occur in the event of a disaster where the
20 backbone network is destroyed. The rescue teams (e.g. firemen
and police officers) would have to communicate directly with
each other without a backbone network in order to provide
disaster recovery.

25

Summary of the invention

In one embodiment, a communication terminal of a cellular
mobile communication system is provided, the cellular mobile
30 communication system comprising the communication terminal,
another communication terminal and a communication network
for providing a communication connection between the
communication terminal and the other communication terminal

via at least one base station of the communication network,
the communication terminal comprising a determiner configured
to determine an encryption key for secure communication
between the communication terminal and the other
5 communication terminal via a radio interface between the
communication terminal and the other communication terminal
and a transceiver configured to perform secure communication
with the other communication terminal via the radio interface
between the communication terminal and the other
10 communication terminal using the determined encryption key.

According to another embodiment, a method for performing
communication according to the communication terminal
described above is provided.

15

Short description of the figures

Illustrative embodiments of the invention are explained below
20 with reference to the drawings.

Figure 1 shows a communication terminal according to an
embodiment.

25 Figure 2 shows a flow diagram according to an embodiment.

Figure 3 shows a communication system according to an
embodiment.

30 Figure 4 shows a message flow diagram according to an
embodiment.

Figure 5 shows a flow diagram according to an embodiment.

Figure 6 shows a communication arrangement according to an embodiment.

5 Figure 7 shows a message flow diagram according to an embodiment.

Figure 8 shows a flow diagram according to an embodiment.

10 Figure 9 shows a communication arrangement according to an embodiment.

Figure 10 shows a message flow diagram according to an embodiment.

15

Figure 11 shows a flow diagram according to an embodiment.

Figure 12 shows a flow diagram according to an embodiment.

20 Figure 13 shows a message flow diagram according to an embodiment.

Figure 14 shows a flow diagram according to an embodiment.

25 Figure 15 shows a message flow diagram according to an embodiment.

Figure 16 shows a message flow diagram according to an embodiment.

30

Detailed description

According to one embodiment, a communication terminal as
5 illustrated in figure 1 is provided.

Figure 1 shows a communication terminal 101 according to an
embodiment.

10 The communication terminal 101 is a (mobile) communication
terminal of a cellular mobile communication system 100. The
cellular mobile communication system 100 comprises the
communication terminal 101, another communication terminal
102 and a communication network 103 for providing a
15 communication connection between the communication terminal
and the other communication terminal via at least one base
station 104 of the communication network.

The communication terminal 101 comprises a determiner 105
20 configured to determine an encryption key for secure
communication between the communication terminal 101 and the
other communication terminal 102 via a radio interface 107
between the communication terminal 101 and the other
communication terminal 102.

25 The communication terminal 101 further comprises a
transceiver 106 configured to perform secure communication
with the other communication terminal 101 via the radio
interface 107 between the communication terminal 101 and the
30 other communication terminal 102 using the determined
encryption key.

According to one embodiment, in other words, a communication terminal of a cellular mobile communication network provides a key for a direct communication between the communication terminal and another communication terminal, i.e. a

5 communication without involvement of the network side, e.g. without involvement of any base station of the communication network. For example, the communication terminal may negotiate the key with the other communication terminal. This negotiation may also take place via a direct communication.

10

According to an embodiment the secure communication is direct communication between the communication terminal and the other communication terminal.

15 According to an embodiment the direct communication is communication of data without the data being communicated via a base station of the communication network.

Direct communication is for example communication of data
20 without the communication network being involved in the communication.

According to an embodiment the determiner is configured to determine the encryption key by exchanging messages with the
25 other communication terminal via the radio interface between the communication terminal and the other communication terminal.

According to an embodiment the messages are exchanged via
30 direct communication between the communication terminal and the other communication terminal.

The messages are for example exchanged between the communication terminal and the other communication terminal without being communicated via a base station of the communication network.

5

The messages are for example exchanged between the communication terminal and the other communication terminal without the communication network being involved in the exchange of the messages.

10

According to an embodiment the communication network is a communication network according to a 802.16 communication standard.

15 The communication network is for example a communication network according to the 802.16n communication standard.

According to an embodiment the transceiver is configured to send a request for a direct communication with the other
20 communication terminal to the communication network or to the other communication terminal.

The transceiver may be configured to include a certificate into the request.

25

The transceiver may be configured to include a nonce into the request.

According to an embodiment the transceiver is configured to
30 receive the encryption key from the communication network or from the other communication terminal and wherein the determiner is configured to determine the encryption key as the received encryption key.

The transceiver may for example be configured to receive the encryption key with a message from the communication network or the other communication terminal and is configured to
5 authenticate the message.

The transceiver is for example configured to check the message for message freshness.

10 According to an embodiment the transceiver is configured to send a message including the determined encryption key to the communication network or to the other communication terminal.

The transceiver may be configured to include a certificate
15 into the request.

The transceiver may be configured to include a nonce into the request.

20 According to an embodiment the communication terminal is configured to act as a base station of the communication network.

According to an embodiment the determiner is configured to
25 determine the encryption key based on a pre-shared encryption key which was pre-shared between the communication terminal and the other communication terminal.

The communication terminal 100 for example carries out a
30 method as illustrated in figure 2.

Figure 2 shows a flow diagram 200 according to an embodiment.

The flow diagram 200 illustrates a method for setting up a communication between a communication terminal of a cellular mobile communication system and another communication terminal of the cellular mobile communication system, the cellular mobile communication system comprising the communication terminal, the other communication terminal and a communication network for providing a communication connection between the communication terminal and the other communication terminal via at least one base station of the communication network.

In 201, an encryption key for secure communication between the communication terminal and the other communication terminal via a radio interface between the communication terminal and the other communication terminal is determined.

In 202, secure communication between the communication terminal and the other communication terminal is performed via the radio interface between the communication terminal and the other communication terminal using the determined encryption key.

It should be noted that embodiments described in context of the communication terminal are analogously valid for the method for performing communication and vice versa.

As mentioned above, the communication network is for example a communication network according to a 802.16 communication standard. The current 802.16 standards do not provide security protocols for the direct communications scenario.

According to one embodiment, in order to ensure that an attacker is not able to eavesdrop into the direct

communications and/or impersonate a HR-MS (i.e. a mobile terminal) in the network, security protocols for authentication and key exchange in the 802.16n network are designed. The 802.16n SRD (System Requirements Document) specifies two scenarios for security, namely Network Aided Mutual Authentication of HR-MS and Data Security and Autonomous (limited) Mutual Authentication of HR-MS and Data Security for Direct Communications.

10 In the following AKE (Authenticated Key Exchange) protocols for the Network Aided Mutual Authentication of HR-MS (i.e. mobile stations according to IEEE 802.16n) and Data Security and Autonomous Mutual Authentication of HR-MS and Data Security for Direct Communications according to various
15 embodiments are described. It should be noted that it is assumed in the examples described below that a node (i.e. a mobile stations or a base station) shall resend a message after timeout if the node did not receive any response to the message. According to one embodiment, once the maximum number
20 of resends is reached, then the node shall stop the protocol or initiate another instance of the protocol.

In the following description, a sending operation of a message from a sender to a receiver is written as

25 sender→receiver: message

Further, in the description of the content of a message, the symbol '|' is used to denote concatenation.

30 With reference to figures 3, 4 and 5, Network Aided Mutual Authentication of HR-MS and Data Security according to one embodiment is described.

Figure 3 shows a communication system 300 according to an embodiment.

The communication system 300 comprises a first mobile terminal (also referred to as HR-MS1) 301, a second mobile terminal (also referred to as HR-MS2) 302 and a communication network (also referred to as network side of the communication system 300) comprising a base station (also referred to as HS-BS) 303 and a backbone network 304.

The communication system 300 is for example a communication system according to a 802.16 standard, i.e. a IEEE 802.16 standard.

In normal operation, the base station 303 provides coverage for the mobile terminals 301, 302 such that the mobile terminals 301, 302 can communicate via the base station 303.

It is supposed that HR-MS1 301 wishes to establish a direct communication pre-shared key with HR-MS2 302 so that HR-MS1 301 and HR-MS2 302 can communicate with each other directly in the event of a backbone (i.e. backbone network 304) failure (i.e. in case that there is no HR-BS 103 around to provide a communication connection via the network side).

For this, according to one embodiment, the protocol as illustrated in figures 4 and 5 is followed to establish the direct communication pre-shared key DMK.

Figure 4 shows a message flow diagram 400 according to an embodiment.

The message flow takes place between a first mobile terminal 401 corresponding to the first mobile terminal 301, a second mobile terminal 402 corresponding to the second mobile terminal 302 and a base station 403 corresponding to the base station 303.

The various protocol steps are shown in more detail in figure 5.

Figure 5 shows a flow diagram 500 according to an embodiment.

Step 501: HR-MS1 selects a nonce N_{HR-MS1} , computes

$\theta_{HR-MS1} = MAC_{CMAC1}("DC_REQ_MS" |$

$T_{HR-MS1} | N_{HR-MS1} | HR - MS1Addr | HR - MS2Addr)$ and sends, in

404, a DC_Request_MSG#1 message 405 to HR-BS 503 to request a direct communication pre-shared key DMK to be shared with HR-MS2 502.

$HR - MS1 \rightarrow HR - BS : DC_Request_MSG\#1 \quad (1)$

where

DC_Request_MSG#1 =

"DC_REQ_MS" | $T_{HR-MS1} | N_{HR-MS1} | HR - MS1Addr | HR - MS2Addr |$

θ_{HR-MS1} .

It should be noted that MAC_{CMAC1} refers to the MAC (Message Authentication Code) generated by MS1 using its CMAC key (i.e. CMAC1). MAC_{CMAC2} refers to the MAC (Message Authentication Code) generated by MS2 using its CMAC key (i.e. CMAC2). MAC_{DCMAC} refers to the MAC (Message Authentication Code) generated by MS1 and/or using its shared CMAC key (i.e. DCMAC)

Step 502: HR-BS 503 checks T_{HR-MS1} , N_{HR-MS1} for message freshness and θ_{HR-MS1} for message authentication. If the verifications are correct, HR-BS selects N_{HR-BS} , computes $\theta_{HR-BS} = \text{MAC}_{\text{CMAC2}}("DC_REQ_BS" \mid T_{HR-BS} \mid N_{HR-BS} \mid \text{HR} - \text{MS1Addr} \mid \text{HR} - \text{MS2Addr})$ and sends, in 406, a DC_Request_MSG#2 message 407 to HR-MS2 502 to inform HR-MS2 502 of the direct connection request from HR-MS1 501.

HR - BS $\rightarrow$ HR - MS2 : DC_Request_MSG#2 (2)

10

where

DC_Request_MSG#2 =
 "DC_REQ_BS" $\mid T_{HR-BS} \mid N_{HR-BS} \mid \text{HR} - \text{MS1Addr} \mid \text{HR} - \text{MS2Addr} \mid \theta_{HR-BS}$.

15 Step 503: HR-MS2 402 checks T_{HR-BS} , N_{HR-BS} for message freshness and θ_{HR-BS} for message authentication. If the verifications are correct, HR-MS2 402 selects N_{HR-MS2} , computes $\theta_{HR-MS2} = \text{MAC}_{\text{CMAC2}}("DC_REPLY_MSG" \mid T_{HR-MS2} \mid N_{HR-MS2} \mid \text{HR} - \text{MS1Addr} \mid \text{HR} - \text{MS2Addr} \mid N_{HR-BS})$ and sends, in 408, a DC_REPLY_MSG#3 message 409 to HR-BS 403 to inform HR-BS 403 of its decision to directly communication with HR-MS1 401.

25 HR - MS2 $\rightarrow$ HR - BS : DC_REPLY_MSG#3 (3)

where

DC_REPLY_MSG#3 = "DC_REPLY_MSG" $\mid T_{HR-MS2} \mid N_{HR-MS2} \mid \text{HR} - \text{MS1Addr} \mid \text{HR} - \text{MS2Addr} \mid N_{HR-BS} \mid \theta_{HR-MS2}$. Note that

"DC_REPLY_MSG" = "DC_REPLY_OK" if HR-MS2 402 agrees for
 30 direct communications with HR-MS1 401 and "DC_REPLY_MSG" =

"DC_REPLY_NOTOK" if HR-MS2 402 refuses direct communications with HR-MS1 401.

Step 504: HR-BS 403 checks T_{HR-MS2} , N_{HR-MS2} for message
 5 freshness and θ_{HR-MS2} for message authentication. If the
 verifications are correct, HR-BS 403 checks the response from
 HR-MS2 402. If "DC_REPLY_MSG" = "DC_REPLY_NOTOK", then the
 protocol stops and HR-BS selects $N_{HR-BS'}$, computes
 $\theta_{HR-BS'} = \text{MAC}_{\text{CMAC1}}(\text{"DC_REPLY_NOK_BS"} \mid T_{HR-BS'} \mid N_{HR-BS'} \mid N_{HR-MS1})$
 10 and sends, in 410, a DC_REPLY_MSG#4 message 411 to HR-MS1
 401:

$$\text{HR} - \text{BS} \rightarrow \text{HR} - \text{MS1} : \text{DC_REPLY_MSG\#4} \quad (4)$$

15 where
 $\text{DC_REPLY_MSG\#4} =$
 $\text{"DC_REPLY_NOK_BS"} \mid T_{HR-BS'} \mid N_{HR-BS'} \mid N_{HR-MS1} \mid \theta_{HR-BS'}.$

Otherwise, If "DC_REPLY_MSG" = "DC_REPLY_OK", then HR-BS 403
 20 generates DMK, selects $N_{HR-BS'}$ and encrypts
 $E_{HR-MS1_KEK}(\text{DMK}, \text{key_lifetime}, \text{HR} - \text{MS1Addr}, \text{HR} - \text{MS2Addr})$ and
 computes
 $\theta_{HR-BS'} =$
 $\text{MAC}_{\text{CMAC1}}(\text{"DC_REPLY_OK_BS"} \mid T_{HR-BS'} \mid N_{HR-BS'} \mid E_{HR-MS1_KEK}(\text{DMK},$
 $\text{key_lifetime}, \text{HR} - \text{MS1Addr}, \text{HR} - \text{MS2Addr}) \mid \text{HR} - \text{MS1Addr} \mid$
 25 $\text{HR} - \text{MS2Addr} \mid N_{HR-MS1})$ and sends, in 410, a DC_REPLY_MSG#5
 message 412 to HR-MS1 401:

$$\text{HR} - \text{BS} \rightarrow \text{HR} - \text{MS1} : \text{DC_REPLY_MSG\#5} \quad (5)$$

where

DC_REPLY_MSG#5 =

"DC_REPLY_OK_BS" | T_{HR-BS}' | N_{HR-BS}' | $E_{HR-MS1_KEK}(DMK,$
 $key_lifetime, HR - MS1Addr, HR - MS2Addr)$ | $HR - MS1Addr$ |
 5 $HR - MS2Addr$ | N_{HR-MS1} | θ_{HR-BS}' .

HR-BS 403 also encrypts $E_{HR-MS2_KEK}(DMK, key_lifetime,$
 $HR - MS2Addr, HR - MS1Addr)$ and computes

$\theta_{HR-BS}'' =$

MAC_{CMAC2}("DC_REPLY_OK_BS" | T_{HR-BS}'' | N_{HR-BS} | $E_{HR-MS2_KEK}(DMK,$
 10 $key_lifetime, HR - MS2Addr, HR - MS1Addr)$ | $HR - MS2Addr$ |
 $HR - MS1Addr$ | N_{HR-MS2}) and sends, in 413, a DC_REPLY_MSG#6
 message 414 to HR-MS2 402:

$HR - BS \rightarrow HR - MS2 : DC_REPLY_MSG\#6$ (6)

15 where

DC_REPLY_MSG#6 =

"DC_REPLY_OK_BS" | T_{HR-BS}'' | N_{HR-BS} | $E_{HR-MS2_KEK}(DMK,$
 $key_lifetime, HR - MS2Addr, HR - MS1Addr)$ | $HR - MS2Addr$ |
 $HR - MS1Addr$ | N_{HR-MS2} | θ_{HR-BS}'' .

20

Step 505:

a) HR-MS1 401 first checks T_{HR-BS}' , N_{HR-BS}' and N_{HR-MS1} for
 freshness and θ_{HR-BS}' for message authentication. If the
 verifications are correct, then HR-MS1 decrypts

25 $E_{HR-MS1_KEK}(DMK, key_lifetime, HR - MS1Addr, HR - MS2Addr)$ and
 obtains DMK and its lifetime $key_lifetime$.

b) HR-MS2 first checks T_{HR-BS}'' , N_{HR-BS} and N_{HR-MS2} for
 freshness and θ_{HR-BS}'' for message authentication. If the

30 verifications are correct, then HR-MS2 decrypts

E_{HR-MS2}_KEK(DMK, key_lifetime, HR - MS2Addr, HR - MS1Addr) and obtains DMK and its lifetime key_lifetime.

The attributes of the messages 405, 407, 409, 411, 412, 414 are summarized in the following tables.

Table 1: DC_Request_MSG#1 message attribute

Notation	Meaning
"DC_REQ_MS"	Direct communication request sent from HR-MS1
T _{HR-MS1}	Timestamp generated by HR-MS1
N _{HR-MS1}	Freshly generated random number of 64bits by HR-MS1
HR - MS1Addr	Address of HR-MS1
HR - MS2Addr	Address of HR-MS1
θ_{HR-MS1}	Message digest calculated using DCMAC key by HR-MS1

10

Table 2: DC_Request_MSG#2 message attribute

Notation	Meaning
"DC_REQ_BS"	Direct communication request sent to HR-MS2 by HR-BS
T _{HR-BS}	Timestamp generated by HR-BS
N _{HR-BS}	Freshly generated random number of 64bits by HR-BS
HR - MS1Addr	Address of HR-MS1
HR - MS2Addr	Address of HR-MS2

θ_{HR-BS}	Message digest calculated using DCMAC key by HR-BS
------------------	--

Table 3: DC_REPLY_MSG#3 message attribute

Notation	Meaning
"DC_REPLY_MSG"	"DC_REPLY_MSG" = "DC_REPLY_OK" if HR-MS2 agrees to direct communications with HR-MS1. "DC_REPLY_MSG" = "DC_REPLY_NOTOK" if HR-MS2 refuses direct communications with HR-MS1.
T_{HR-MS2}	Timestamp generated by HR-MS2
N_{HR-MS2}	Freshly generated random number of 64bits by HR-MS2
HR - MS1Addr	Address of HR-MS1
HR - MS2Addr	Address of HR-MS2
N_{HR-BS}	Nonce generated by HR-BS
θ_{HR-MS2}	Message digest calculated using DCMAC key by HR-MS2

5

Table 4: DC_REPLY_MSG#4 message attribute for rejection of Direct Communications

Notation	Meaning
"DC_REPLY_NOK_BS"	HR-BS response to HR-MS1 that HR-MS2 rejected direct communications
$T_{HR-BS'}$	Timestamp generated by HR-MS2
$N_{HR-BS'}$	Freshly generated random number of 64bits by HR-MS2
N_{HR-MS1}	Nonce generated by HR-MS1

$\theta_{HR-BS'}$	Message digest calculated using DCMAC key by HR-BS
-------------------	--

Table 5: DC_REPLY_MSG#5 message attribute for
Acceptance of Direct Communications

Notation	Meaning
"DC_REPLY_OK_BS"	HR-BS response to HR-MS1 that HR-MS2 accepted direct communications
$T_{HR-BS'}$	Timestamp generated by HR-BS
$N_{HR-BS'}$	Freshly generated random number of 64bits by HR-BS
$E_{HR-MS1_KEK}(DMK, key_lifetime, HR - MS1Addr, HR - MS2Addr)$	Encryption of DMK, key lifetime by HR-BS using HR-MS1's KEK
HR - MS1Addr	Address of HR-MS1
HR - MS2Addr	Address of HR-MS2
N_{HR-MS1}	Nonce generated by HR-MS1
$\theta_{HR-BS'}$	Message digest calculated using DCMAC key by HR-BS

Table 6: DC_REPLY_MSG#6 message attribute for
Acceptance of Direct Communications

Notation	Meaning
"DC_REPLY_OK_BS"	HR-BS OK response to HR-MS2 for the direct communications
T_{HR-BS}	Timestamp generated by HR-BS
N_{HR-BS}	Nonce generated by HR-BS
$E_{HR-MS2_KEK}(DMK, key_lifetime, HR-MS2Addr, HR-MS1Addr)$	Encryption of DMK, key lifetime by HR-BS using HR-MS2's KEK
$HR-MS2Addr$	Address of HR-MS2
$HR-MS1Addr$	Address of HR-MS1
N_{HR-MS2}	Nonce generated by HR-MS2
θ_{HR-BS}	Message digest calculated using DCMAC key by HR-BS

5

In the following, with reference to figures 6 to 12, three AKE protocols for Mutual Authentication of HR-MS and data security for Direct Communications according to various embodiments are described. The three protocols are designed to address the three scenarios, namely 1) PKI scenario (figure 6, 7 and 8), where it is assumed each HR-MS has a digital certificate to assist in the AKE protocol, 2) HR-MS convert to HR-BS* scenario (figures 9, 10 and 11), which covers the multimode HR-mode capabilities and 3) Pre-shared

10

15

key scenario (figures 6, 16 and 12), where it is assumed that HR-MS1 and HR-MS2 shares a key prior to direct communications. It should be noted that according to one embodiment, all messages have a MaxResends and a Message Timeout. When a node (e.g. a HR-MS or a HR-BS) does not receive a response message to a message that it has sent from another node within the Message Timeout time, then the node resends its message. If the MaxResends number is reached for the message then it initiates another round of authentication or drops the direct communication.

Firstly, the PKI approach according to one embodiment is described with reference to figures 6, 7 and 8.

Figure 6 shows a communication arrangement 600 according to an embodiment.

Similarly to the communication system 300 shown in figure 3, the communication system 600 comprises a first mobile terminal (also referred to as HR-MS1) 601, a second mobile terminal (also referred to as HR-MS2) 602 and a communication network (also referred to as network side of the communication system 600) comprising a base station (also referred to as HS-BS) 603 and a backbone network 604.

The communication system 600 is for example a communication system according to a IEEE 802.16 standard.

In normal operation, the base station 603 provides coverage for the mobile terminals 601, 602 such that the mobile terminals 601, 602 can communicate via the base station 603.

For this embodiment, it is assumed that the base station 603 is not available for providing communication between the mobile terminals 601, 602. For example, the backbone network 604 has failed. In this scenario, it is assumed that each.

5 mobile terminal 601, 602 has a digital certificate issued by a certification authority for mutual authentication and key exchange.

10 Figure 7 shows a message flow diagram 700 according to an embodiment.

The message flow takes place between a first mobile terminal 701 corresponding to the first mobile terminal 601 and a second mobile terminal 702 corresponding to the second mobile terminal 602.

The various protocol steps are shown in more detail in figure 8.

20 Figure 8 shows a flow diagram 800 according to an embodiment.

Step 801: HR-MS1 701 first generates a nonce N_{HR-MS1} . Next, HR-MS1 701, in 703, computes the signature

$\sigma_{HR-MS1} = \text{SIGN}(T_{HR-MS1} \parallel N_{HR-MS1} \parallel HR - MS2Addr \parallel HR - MS1Addr)$

25 and sends, in 704, a DirectComms_KeyAgreement_MSG_#1 message 705 to HR-MS2 702:

"HR - MS1" → "HR - MS2" : DirectComms_KeyAgreement_MSG_#1 (7)

30 where

DirectComms_KeyAgreement_MSG_#1 =

$T_{HR-MS1} \parallel N_{HR-MS1} \parallel HR - MS2Addr \parallel HR - MS1Addr \parallel$

$\sigma_{HR-MS1} \parallel \text{Cert}(HR - MS1)$. DirectComms_KeyAgreement_MSG_#1 is

also known as PKIDirectComms_KeyAgreement_MSG_#1 in P802.16n (802.16e based) and Peer_KeyAgreement_MSG_#1 in P802.16.1a (802.16m based).

- 5 Step 802: HR-MS2 702 first verifies the received timestamp and nonce for freshness and the certificate $\text{Cert}(\text{HR} - \text{MS1})$ and signature $\sigma_{\text{HR-MS1}}$ in 706. If the verifications are correct, then HR-MS2 generates a nonce $N_{\text{HR-MS2}}$ and DMK and computes
- 10 $\text{DAK} = \text{Dot16KDF}(\text{DMK}, \text{HR} - \text{MS1Addr} \parallel \text{HR} - \text{MS2Addr} \parallel \text{"DAK"}, 160)$ and the $\text{DCMAC} = \text{Dot16KDF}(\text{DAK}, \text{"DCMAC_KEYS"}, 128)$ and
- $\text{DTEK} = \text{DOT16KDF}(\text{DAK}, \text{"DTEK_KEY"}, 128)$ and
- $\theta_{\text{HR-MS2}} = \text{MAC}_{\text{DCMAC}}(N_{\text{HR-MS2}} \parallel N_{\text{HR-MS1}} \parallel \text{HR} - \text{MS2Addr} \parallel \text{HR} - \text{MS1Addr})$ in 707.
- HR-MS2 then uses HR-MS1's public key to encrypt and obtain
- 15 $E_{\text{HR-MS1_K}}(\text{DMK}, \text{key_lifetime}, \text{HR} - \text{MS1Addr}, \text{HR} - \text{MS2Addr})$.
- Finally, in 708, the HR-MS2 702 computes signature
- $\sigma_{\text{HR-MS2}} = \text{SIGN}(T_{\text{HR-MS2}} \parallel$
- $N_{\text{HR-MS2}} \parallel \text{HR} - \text{MS1Addr} \parallel \text{HR} - \text{MS2Addr} \parallel N_{\text{HR-MS1}} \parallel$
- $E_{\text{HR-MS1_K}}(\text{DMK}, \text{key_lifetime}, \text{HR} - \text{MS1Addr},$
- 20 $\text{HR} - \text{MS2Addr}) \parallel \theta_{\text{HR-MS2}})$ and sends, in 709, a
- DirectComms_KeyAgreement_MSG_#2 message 710 to HR-MS1 701:

$\text{HR} - \text{MS2} \rightarrow \text{HR} - \text{MS1} : \text{DirectComms_KeyAgreement_MSG_}\#2 \quad (8)$

- 25 where
- DirectComms_KeyAgreement_MSG_#2 =
- $T_{\text{HR-MS2}} \parallel N_{\text{HR-MS2}} \parallel \text{HR} - \text{MS1Addr} \parallel \text{HR} - \text{MS2Addr} \parallel$
- $N_{\text{HR-MS1}} \parallel E_{\text{HR-MS1_K}}(\text{DMK}, \text{key_lifetime}, \text{HR} - \text{MS1Addr}, \text{HR} - \text{MS2Addr}) \parallel$
- $\theta_{\text{HR-MS2}} \parallel \sigma_{\text{HR-MS2}} \parallel \text{Cert}(\text{HR} - \text{MS2}).$
- 30 DirectComms_KeyAgreement_MSG_#2 is also known as
- PKIDirectComms_KeyAgreement_MSG_#2 in P802.16n (802.16e

based) and Peer_KeyAgreement_MSG_#2 in P802.16.1a (802.16m based)

Step 803: HR-MS1 701 first verifies the received timestamp and nonces for freshness and the certificate $\text{Cert}(\text{HR} - \text{MS2})$ and signature $\sigma_{\text{HR-MS2}}$ in 711. If the verifications are correct, then HR-MS1 701 decrypts

$E_{\text{HR-MS1}} \text{_PK}(\text{DMK}, \text{key_lifetime}, \text{HR} - \text{MS1Addr}, \text{HR} - \text{MS2Addr})$ and obtains DMK and key_lifetime. Next, HR-MS1 701 computes DAK,

DCMAC and DTEK and verifies $\theta_{\text{HR-MS2}}$ in 712 and 713. If the verification is correct, then HR-MS1 701 computes

$\theta_{\text{HR-MS1}} = \text{MAC}_{\text{DCMAC}}(\text{N}_{\text{HR-MS1}} \parallel \text{N}_{\text{HR-MS2}} \parallel \text{HR} - \text{MS1Addr} \parallel \text{HR} - \text{MS2Addr})$ and sends, in 714, a DirectComms_KeyAgreement_MSG_#3 message

715:

15

$\text{HR} - \text{MS1} \rightarrow \text{HR} - \text{MS2} : \text{DirectComms_KeyAgreement_MSG_}\#3 \quad (9)$

where

DirectComms_KeyAgreement_MSG_#3 =

20 $\text{N}_{\text{HR-MS2}} \parallel \text{HR} - \text{MS2Addr} \parallel \text{HR} - \text{MS1Addr} \parallel \theta_{\text{HR-MS1}}.$

DirectComms_KeyAgreement_MSG_#3 is also known as

PKIDirectComms_KeyAgreement_MSG_#3 in P802.16n (802.16e based) and Peer_KeyAgreement_MSG_#3 in P802.16.1a (802.16m based)

25

Step 804: HR-MS2 702 receives the

DirectComms_KeyAgreement_MSG_#3 message 715 and verifies the received nonce and the CMAC tuple in 716. If the verification is correct, then HR-MS2 702 confirms that HR-MS1 701 has computed the correct keys and commences secure direct communications in 717 and 718.

30

The attributes of the messages 704, 706, 708 are summarized in the following tables.

5 Table 7: DirectComms_KeyAgreement_MSG_#1 message attribute

Notation	Meaning
T_{HR-MS1}	Timestamp generated by HR-MS1. T_{HR-MS1} is also known as HR_MS1_Timestamp in P802.16n (802.16e based) and also known as Timestamp_HR-MS1 in P802.16.1a (802.16m based)
N_{HR-MS1}	Freshly generated random number of 64bits by HR-MS1. N_{HR-MS1} is also known as HR_MS1_Random in P802.16n (802.16e based) and also known as NONCE_HR-MS1 in P802.16.1a (802.16m based)
HR - MS2Addr	Address of HR-MS2
HR - MS1Addr	Address of HR-MS1
σ_{HR-MS1}	Signature of message generated by HR-MS1 using its RSA private key. σ_{HR-MS1} is also known as sigHR-MS1 in P802.16n (802.16e based) and P802.16.1a (802.16m based).
Cert(HR - MS1)	Digital certificate of HR-MS1. Cert(HR-MS1) is also known as HR-MS1_Certificate in P802.16n (802.16e based) and P802.16.1a (802.16m based).

10 Table 8: DirectComms_KeyAgreement_MSG_#2 message attribute

Notation	Meaning
----------	---------

T_{HR-MS2}	Timestamp generated by HR-MS2. T_{HR-MS2} is also known as HR_MS2_Timestamp in P802.16n (802.16e based) and also known as Timestamp_HR-MS2 in P802.16.1a (802.16m based)
N_{HR-MS2}	Freshly generated random number of 64bits by HR-MS2. N_{HR-MS2} is also known as HR_MS2_Random in P802.16n (802.16e based) and also known as NONCE_HR-MS2 in P802.16.1a (802.16m based)
HR - MS1Addr	Address of HR-MS1
HR - MS2Addr	Address of HR-MS2
N_{HR-MS1}	Nonce generated by HR-MS1 in DirectComms_KeyAgreement_MSG_#1 message
$E_{HR-MS1_PK}(DMK, key_lifetime, HR - MS1Addr, HR - MS2Addr)$	Public key encryption using HR-MS1's Public key where DMK = DirectComms Master Key generated by HR-MS and key_lifetime = lifetime of DMK. $E_{HR-MS1_PK}(DMK, key_lifetime, HR - MS1Addr, HR - MS2Addr)$ can also be written as Encrypted DMK in P802.16n (802.16e based) and P802.16.1a (802.16m based)
θ_{HR-MS2}	Message digest calculated using DCMAC key by HR-MS2. θ_{HR-MS2} is also known as HR-MS2_CMAC in P802.16n (802.16e

	based) and also known as CMAC_HR-MS2 in P802.16.1a (802.16m based)
$\sigma_{\text{HR-MS2}}$	Signature of message generated by HR-MS2 using its RSA private key $\sigma_{\text{HR-MS2}}$ is also known as sigHR-MS2 in P802.16n (802.16e based) and P802.16.1a (802.16m based).
Cert(HR - MS2)	Digital certificate of HR-MS2. Cert(HR-MS2) is also known as HR-MS2_Certificate in P802.16n (802.16e based) and P802.16.1a (802.16m based).

Table 9: DirectComms_KeyAgreement_MSG_#3 message attribute

Notation	Meaning
$N_{\text{HR-MS2}}$	Nonce generated by HR-MS2 in DirectComms_KeyAgreement_MSG_#2 message
HR - MS2Addr	Address of HR-MS2
HR - MS1Addr	Address of HR-MS1
$\theta_{\text{HR-MS1}}$	Message digest calculated using DCMAC key by HR-MS1. $\theta_{\text{HR-MS1}}$ is also known as HR-MS1_CMAL in P802.16n (802.16e based) and also known as CMAC_HR-MS1 in P802.16.1a (802.16m based)

In the following, the approach for the scenario that one of the mobile terminals converts into a base station according to one embodiment is described with reference to figures 9, 10 and 11.

5

Figure 9 shows a communication arrangement 900 according to an embodiment.

Similarly to the communication system 300 shown in figure 3,
10 the communication system 900 comprises a first mobile terminal (also referred to as HR-MS1) 901, a second mobile terminal (also referred to as HR-MS2) 902 and a communication network (also referred to as network side of the communication system 900) comprising a base station (also
15 referred to as HS-BS) 903 and a backbone network 904.

The communication system 900 is for example a communication system according to a IEEE 802.16 standard.

20 In normal operation, the base station 903 provides coverage for the mobile terminals 901, 902 such that the mobile terminals 901, 902 can communicate via the base station 903.

For this embodiment, it is assumed that the base station 903
25 is not available for providing communication between the mobile terminals 901, 902. For example, the backbone network 904 has failed.

In this scenario, it is assumed that the HR-MS1 converts to a
30 base station (referred to as HR-BS*) 905 in order to establish a secure direct communication channel with HR-MS2 902. The AKE protocol used according to this embodiment is

described in the following with reference to figures 10 and 11.

Figure 10 shows a message flow diagram 1000 according to an embodiment.

The message flow takes place between a first mobile terminal 1001 corresponding to the first mobile terminal 901 which is converted to a base station HR-BS* and a second mobile terminal 1002 corresponding to the second mobile terminal 902.

The various protocol steps are shown in more detail in figure 11.

Figure 11 shows a flow diagram 1100 according to an embodiment.

Step 1101: The first mobile terminal 901 converts to HR-BS* 905, 1001.

Step 1102: In 1003, the transformed HR-BS* 1001 sends a DirectComms_KeyAgreement_MSG_#1 message 1004 to HR-MS2 1002:

HR - BS* → HR - MS2 : DirectComms_KeyAgreement_MSG_#1 (10)
where DirectComms_KeyAgreement_MSG_#1 = Cert(HR - BS*).

Step 1103: HR-MS2 1002 first verifies the certificate Cert(HR - BS*). If the verifications are correct, then HR-MS2 generates a nonce N_{HR-MS2} . Next, HR-MS2 1002 computes the signature

$\sigma_{HR-MS2} = \text{SIGN}(T_{HR-MS2} \parallel N_{HR-MS2} \parallel \text{HR - BS}^* \text{ Addr} \parallel \text{HR - MS2 Addr})$

and sends, in 1005, a DirectComms_KeyAgreement_MSG_#2 message 1006 to HR-BS* 1001:

HR - MS2 $\rightarrow$ HR - BS* : DirectComms_KeyAgreement_MSG_#2 (11)

5

where

DirectComms_KeyAgreement_MSG_#2 =

$T_{HR-MS2} \mid N_{HR-MS2} \mid HR - BS * Addr \mid HR - MS2Addr \mid$

$\sigma_{HR-MS2} \mid Cert(HR - MS2).$

10

Step 1104: HR-BS* 1001 first verifies the received timestamp and nonce for freshness and certificate $Cert(HR - MS2)$ and signature σ_{HR-MS2} . If the verifications are correct, then HR-BS* 1001 generates a nonce N_{HR-BS*} and DMK and computes

15 DAK = Dot16KDF(DMK, $HR - BS * Addr \mid HR - MS2Addr \mid "DAK", 160$),
the DCMAC = Dot16KDF(DAK, "DCMAC_KEYS", 128), the
DTEK = DOT16KDF(DAK, "DTEK_KEY", 128) and

$\theta_{HR-BS*} = MAC_{DCMAC}(N_{HR-BS*} \mid N_{HR-MS2} \mid HR - BS * Addr \mid$

$HR - MS2Addr)$. HR-BS* 1001 then uses HR-MS2's 1002 public key

20 to encrypt and obtain $E_{HR-MS2_PK}(DMK,$
 $key_lifetime, HR - BS * Addr, HR - MS2Addr)$. Finally, HR-BS* 1001
computes signature $\sigma_{HR-BS*} =$

$SIGN(T_{HR-BS*} \mid N_{HR-BS*} \mid HR - MS2Addr \mid HR - BS * Addr \mid$
 $N_{HR-MS2} \mid E_{HR-MS2_PK}(DMK, key_lifetime,$

$HR - BS * Addr, HR - MS2Addr) \mid \theta_{HR-BS*})$ and, in 1007, sends a

25 DirectComms_KeyAgreement_MSG_#3 message 1008 to HR-MS2:

HR - BS* $\rightarrow$ HR - MS2 : DirectComms_KeyAgreement_MSG_#3 (1

where

DirectComms_KeyAgreement_MSG_#3 =

30 $T_{HR-BS*} \mid N_{HR-BS*} \mid HR - MS2Addr \mid HR - BS * Addr \mid N_{HR-MS2} \mid$

$E_{HR-MS2_PK}(DMK, key_lifetime, HR - BS * Addr, HR - MS2Addr) |$
 $\theta_{HR-BS*} | \sigma_{HR-BS*} | Cert(HR - BS^*).$

Step 1105: HR-MS2 1002 first verifies the received timestamp,
 5 nonce and signature σ_{HR-BS^*} . If the verifications are
 correct, then HR-MS2 1002 decrypts

$E_{HR-MS2_PK}(DMK, key_lifetime, HR - BS * Addr, HR - MS2Addr)$ and
 obtains DMK and its lifetime $key_lifetime$. Next, HR-MS2 1102
 computes DAK, DCMAC key and DTEK and verifies θ_{HR-BS^*} . If

10 the verification is correct, then HR-MS2 1102 can compute
 $\theta_{HR-MS2} = MAC_{DCMAC}(N_{HR-MS2} | N_{HR-BS^*} | HR - MS2Addr | HR - BS * Addr)$
 and sends, in 1009, a DirectComms_KeyAgreement_MSG_#4 message
 1010:

15 $HR - MS2 \rightarrow HR - BS^* : DirectComms_KeyAgreement_MSG_#4 \ (13)$

where

$DirectComms_KeyAgreement_MSG_#4 =$
 $N_{HR-BS^*} | HR - BS * Addr | HR - MS2Addr | \theta_{HR-MS2} .$

20

Step 1106: HR-BS* 1001 receives the
 DirectComms_KeyAgreement_MSG_#4 message 1010 and verifies the
 received nonce and CMAC tuple. If the verification are
 successful, then HR-BS* 1001 confirms that HR-MS2 1002 has
 25 computed the correct keys and commences secure direct
 communications.

The attributes of the messages 1004, 1006, 1008, 1010 are
 summarized in the following tables.

30

Table 10: DirectComms_KeyAgreement_MSG_#1 message
 attribute

Notation	Meaning
Cert(HR - BS*)	Digital certificate of HR-BS*

Table 11: DirectComms_KeyAgreement_MSG_#2 message attribute

Notation	Meaning
T_{HR-MS2}	Timestamp generated by HR-MS2
N_{HR-MS2}	Freshly generated random number of 64bits by HR-MS2
HR - BS * Addr	Address of HR-BS*
HR - MS2Addr	Address of HR-MS2
σ_{HR-MS2}	Signature of message generated by HR-MS2 using its RSA private key
Cert(HR - MS2)	Digital certificate of HR-MS2

5

Table 12: DirectComms_KeyAgreement_MSG_#3 message attribute

Notation	Meaning
T_{HR-BS^*}	Timestamp generated by HR-BS*
N_{HR-BS^*}	Freshly generated random number of 64bits by HR-BS*
HR - MS2Addr	Address of HR-MS2
HR - BS * Addr	Address of HR-BS*
N_{HR-MS2}	Nonce generated by HR-MS2 in DirectComms_KeyAgreement_MSG_#2 message
$E_{HR-MS2_PK(DMK, key_lifetime, HR - BS * Addr, HR - MS2Addr)}$	Public key encryption using HR-MS2's Public key where DMK = DirectComms Master Key generated by HR-BS* and

	key_lifetime = lifetime of DMK
θ_{HR-BS^*}	Message digest calculated using DCMAC key by HR-BS*
σ_{HR-BS^*}	Signature of message generated by HR-BS* using its RSA private key
Cert(HR - BS*)	Digital certificate of HR-BS*

Table 13: DirectComms_KeyAgreement_MSG_#4 message attribute

Notation	Meaning
N_{HR-BS^*}	Nonce generated by HR-BS* in DirectComms_KeyAgreement_MSG_#3 message
HR - BS * Addr	Address of HR-BS*
HR - MS2Addr	Address of HR-MS2
θ_{HR-MS2}	Message digest calculated using DCMAC key by HR-MS2

5

In the following, the pre-shared key approach according to one embodiment is described with reference to figures 6, 16 and 12.

- 10 It is assumed that HR-MS1 601, 701 and HR-MS2 602, 702 have already established a pre-shared key DMK using one of the methods previously described, such as with the aid of the Network Infrastructure for example using the approach as described above with reference to figures 3, 4 and 5, or some
 15 other method and wish to communicate directly. Then the AKE protocol described in the following can be used. This example is based on the scenario illustrated in figure 6. The message flow is shown in figure 16.

Figure 16 shows a flow diagram 1600 according to an embodiment.

- 5 The message flow takes place between a first mobile terminal 1601 corresponding to the first mobile terminal 601 and a second mobile terminal 1602 corresponding to the second mobile terminal 602.
- 10 The various protocol steps are shown in more detail in figure 12.

Figure 12 shows a flow diagram 1200 according to an embodiment.

15

Step 1201: In 1603, HR-MS1 1601 selects a nonce N_{HR-MS1} and uses the shared DMK and computes $DAK = \text{Dot16KDF}(\text{DMK}, \text{HR} - \text{MS1Addr} \parallel \text{HR} - \text{MS2Addr} \parallel \text{"DAK"}, 160)$, the $\text{DCMAC} = \text{Dot16KDF}(\text{DAK}, \text{"DCMAC_KEYS"}, 128)$ and

- 20 $\theta_{HR-MS1} = \text{MAC}_{\text{DCMAC}}(N_{HR-MS1} \parallel \text{DMK_Sequence_No} \parallel \text{DAKID} \parallel \text{Key_lifetime})$ and $\text{DTEK} = \text{DOT16KDF}(\text{DAK}, \text{"DTEK_KEY"}, 128)$.

Finally, HR-MS1 1601 sends, in 1604, a $\text{DirectComms_KeyAgreement_MSG_\#1}$ 1605 to HR-MS2 1602:

25

$\text{HR} - \text{MS1} \rightarrow \text{HR} - \text{MS2} : \text{DirectComms_KeyAgreement_MSG_}\#1(14)$

where

- 30 $\text{DirectComms_KeyAgreement_MSG_}\#1 = N_{HR-MS1} \parallel \text{DMK_Sequence_No} \parallel \text{DAKID} \parallel \text{Key_lifetime} \parallel \theta_{HR-MS1}$. $\text{DirectComms_KeyAgreement_MSG_}\#1$ 1605 is also known as $\text{Peer_KeyAgreement_MSG_}\#1$ in P802.16.1a (802.16m based).

Step 1202: In 1606, HR-MS2 1602 first verifies that the received nonce is fresh and, in 1607, uses the shared DMK and computes

5 $DAK = \text{Dot16KDF}(DMK, HR - MS1Addr \parallel HR - MS2Addr \parallel "DAK", 160),$
 $DCMAC = \text{Dot16KDF}(DAK, "DCMAC_KEYS", 128),$
 $DTEK = \text{DOT16KDF}(DAK, "DTEK_KEY", 128)$ and uses DCMAC to check
 θ_{HR-MS1} . If the verification is correct, HR-MS2 1602 selects
 N_{HR-MS2} and computes
 10 $\theta_{HR-MS2} =$
 $MAC_{DCMAC}(N_{HR-MS1} \parallel N_{HR-MS2} \parallel DAKID \parallel DMK_Sequence_No \parallel$
 $DC_Security_Parameters).$

Finally, in 1608, HR-MS2 1602 sends a

15 DirectComms_KeyAgreement_MSG_#2 message 1609 to HR-MS1 1601:

$HR - MS2 \rightarrow HR - MS1 : \text{DirectComms_KeyAgreement_MSG_}\#2(15)$

where

20 $\text{DirectComms_KeyAgreement_MSG_}\#2 =$
 $N_{HR-MS1} \parallel N_{HR-MS2} \parallel DAKID \parallel DMK_Sequence_No \parallel$
 $DC_Security_Parameters \parallel \theta_{HR-MS2}.$
 DirectComms_KeyAgreement_MSG_#2 1609 is also known as
 Peer_KeyAgreement_MSG_#2 in P802.16.1a (802.16m based).

25

Step 1203: In 1610, HR-MS1 1601 receives the
 DirectComms_KeyAgreement_MSG_#2 message 1609 from HR-MS2 1602
 and checks the received nonces for freshness and also checks
 30 DAKID and θ_{HR-MS2} . If the verifications are correct, HR-MS1
 1601 computes

$\theta_{HR-MS1}' =$
 $MAC_{DCMAC}(N_{HR-MS1} \parallel N_{HR-MS2} \parallel DMK_Sequence_No \parallel DC_SAID \parallel$
 $DC_Security_Parameters).$

- 5 Finally, in 1611, HR-MS1 1601 sends a
 DirectComms_KeyAgreement_MSG_#3 message 16012 to HR-MS2 1602:

HR - MS1 $\rightarrow$ HR - MS2 : DirectComms_KeyAgreement_MSG_#3 (16)

- 10 where
 DirectComms_KeyAgreement_MSG_#3 =
 $N_{HR-MS1} \parallel N_{HR-MS2} \parallel DMK_Sequence_No \parallel$
 $DC_SAID \parallel DC_Security_Parameters \parallel \theta_{HR-MS1}'.$
 DirectComms_KeyAgreement_MSG_#3 1612 is also known as
 15 Peer_KeyAgreement_MSG_#3 in P802.16.1a (802.16m based).

- Step 1204: Upon receiving the DirectComms_KeyAgreement_MSG_#3
 message 16012, HR-MS2 1602 checks the received nonces for
 freshness and θ_{HR-MS1}' in 1613. If the verifications are
 20 correct, HR-MS2 1602 applies the negotiated security
 parameters and is ready for direct communications with HR-MS1
 1601 which is started in 1614 and 1615. Otherwise, if
 θ_{HR-MS1}' is invalid, then HR-MS2 1602 ignores the
 DirectComms_KeyAgreement_MSG_#3 message 16012.

- 25 The attributes of the messages 1605, 1609, 16012 according to
 pre-shared key approach are summarized in the following
 tables.

- 30 Table 14: DirectComms_KeyAgreement_MSG_#1 message
 attribute

Notation	Meaning
----------	---------

N_{HR-MS1}	a freshly generated random number of 64 bits. N_{HR-MS1} is also known as HR_MS1_Random in P802.16n (802.16e based) and also known as NONCE_HR-MS1 in P802.16.1a (802.16m based)
DMK_Sequence_No	new DMK sequence number
DAKID	identifies the direct communications authorization key
Key_lifetime	DMK key lifetime
θ_{HR-MS1}	Message digest calculated using DCMAC key. θ_{HR-MS1} is also known as HR-MS1_CMAC in P802.16n (802.16e based) and also known as CMAC_HR-MS1 in P802.16.1a (802.16m based)

Table 15: DirectComms_KeyAgreement_MSG_#2 message attribute

Notation	Meaning
N_{HR-MS1}	Nonce generated by HR-MS1 in DirectComms_KeyAgreement_MSG_#1 message
N_{HR-MS2}	a freshly generated random number of 64 bits. N_{HR-MS2} is also known as HR_MS2_Random in P802.16n (802.16e based) and also known as NONCE_HR-MS2 in P802.16.1a (802.16m based)
DAKID	identifies the direct communications authorization key for protecting this message
DMK_Sequence_No	new DMK sequence number

DC_Security_Parameters	The requesting HR-MS's security capabilities
θ_{HR-MS2}	Message digest calculated using DCMAC key. θ_{HR-MS2} is also known as HR-MS2_CMAC in P802.16n (802.16e based) and also known as CMAC_HR-MS2 in P802.16.1a (802.16m based)

Table 16: DirectComms_KeyAgreement_MSG_#3 message attribute

Notation	Meaning
N_{HR-MS1}	Nonce generated by HR-MS1 in DirectComms_KeyAgreement_MSG_#1 message
N_{HR-MS2}	Nonce generated by HR-MS2 in DirectComms_KeyAgreement_MSG_#2 message
DMK_Sequence_No	new DMK sequence number
DC_SAID	identifies the direct communications authorization key for protecting this message
DC_Security_Parameters	The supporting HR-MS's security capabilities
$\theta_{HR-MS1'}$	Message digest calculated using DCMAC key. $\theta_{HR-MS1'}$ is also known as HR-MS1_CMAC in P802.16n (802.16e based) and also known as CMAC_HR-MS1 in P802.16.1a (802.16m based)

In the following, examples for the derivation of the keys mentioned above are given.

According to one embodiment, the DMK is the security key/pre-established shared key that is randomly generated by HR-BS 303 or HR-MS 301, 302 or a network entity (e.g. an AAA Server etc). According to one embodiment, the DMK is a key (e.g. a 160-bit key) that is randomly generated by HR-BS 303 in the Network-aided Security Procedure described with reference to figures 3, 4 and 5, by HR-MS2 602 in the PKI approach described with reference to figures 6, 7 and 8 and by HR-BS* 905 in the approach in which a HR-MS converts to a HR-BS* of the Autonomous Security Procedure described with reference to figures 9, 10 and 11. According to one embodiment, it is already pre-established in the pre-shared key approach described with reference to figures 6, 16 and 12. According to one embodiment, the DMK is delivered by Key Transfer (EAP) messages.

The DMK may be used as a source for keying materials required by upper layers.

DAK is derived from DMK and belongs to a pair of HR-MSs. The DAK is used for Direct Communications in the event of failure in the backbone.

The DAK derivation is for example done as follows:

$$\text{DAK} = \text{Dot16KDF}(\text{DMK}, \text{HR} - \text{MS1Addr} \mid \text{HR} - \text{MS2Addr} \mid \text{"DAK"}, 160) \quad (17)$$

where:

HR - MS1Addr and HR - MS2Addr are the addresses of HR-MS1 and HR-MS2 respectively.

The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys:

- 5 • Direct Communication Cipher-based Message Authentication Code (DCMAC) key
- Direct Communication Traffic Encryption (DTEK) Key

The DCMAC-DTEK prekey derivation is done as follows:

10

DCMAC-DTEK prekey = Dot16KDF (DAK, DAK_COUNT|"DCMAC-DTEK prekey", 160)

The DCMAC key is derived from DAK and used for message
15 authentication for the messages sent during direct communications.

For example, the DCMAC key is derived as follows:

20 DCMAC = Dot16KDF(DAK, "DCMAC_KEYS", 128) (18)

DCMAC key = Dot16KDF(DCMAC-DTEK prekey, "DCMAC_KEYS",
128)

DTEK is used to transport encryption key used to encrypt data
25 in direct communications.

DTEK is for example derived as follows:

DTEK = Dot16KDF(DAK, "DTEK_KEY", 128) (19)

DTEK = Dot16KDF(DCMAC-DTEK prekey,
30 DSAID|COUNTER_DTEK|"DTEK_KEY", 128)

DSAID is the security association to which the DTEK belongs.

COUNTER_DTEK is a counter used to derive different DTEKs for the same DSAID, the value of the counter is changed everytime a new DTEK needs to be derived within the same DAK and DAK_COUNT pair is valid. Everytime a new DCMAC-DTEK prekey is derived, this counter is reset.

According to one embodiment the PKM messages in the 802.16m and 802.16e standards are modified to support the direct communication security feature in the 802.16n GridMAN standard.

In the following, amendments to Privacy Key Management (PKM) messages in IEEE P802.16.1a according to one embodiment are described.

In the following text changes to the Privacy Key Management (PKM) messages in the P802.16.1a AWD (802.16m standards) to support Security procedure for direct communication data security according to one embodiment are described.

The Privacy Key Management (PKM) messages are located in Section 16.2.3.43 of the 802.16m-2011 standards. The modified Table 726 -AAI-PKM-REQ message field description and Table 727 -AAI-PKM-RSP message field description are according to one embodiment modified as follows:

Table 17: Modified Table 726-AAI-PKM-REQ message field description

Field	Size (bits)	Value/Description	Condition
PKM v3	4	- PKMv3 Reauth-Request; PKM	

message type code		v3 message code = 1 - PKMv3 EAP-Transfer; PKM v3 message code = 2 - PKMv3 Key_Agreement-MSG#2; PKM v3 message code = 4 - PKMv3 TEK-Request; PKM v3 message code = 6 - PKMv3 TEK-Invalid; PKM v3 message code = 8 - Peer_KeyAgreement_MSG #2; PKM v3 message code = 10 12-16: Reserved	
PKM identifier	8	A value used to match an ABS response to the AMS requests or an AMS response to the ABS requests	
CMAC indicator	1	Indicates whether this message is protected by CMAC tuple 0: Not protected 1: Protected	Shall always be present
If(PKM v3 message code ==2) {			
EAP payload	variable (1..14 00 x 8)	Contains the EAP authentication data, not interpreted in the MAC	
}			

If(PKM v3 message code == 4) {			
...			
...			
If(PKM v3 message code == 8) {			
SAID	8	Security association identifier	
}			
If(PKM v3 message code == 10) {			
Key Agreement Type	8	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI 2: BS-to-BS security 3-255: Reserved	
If(Key Agreement Type == 0) {			
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	

DAKID	64	identifies the direct communications authorization key	
size of ICV	1	0: size of ICV = 32 bits (default; Max Invalid value is 4096) 1: size of ICV = 64 bits (Max Invalid value is not used)	
PN window Size	16	The receiver shall track PNs within this window to prevent replay attacks	
}			
If (Key Agreement Type == 1) {			
Timestamp_HR-MS2	32	Timestamp	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
HR-MS1Addr	48	MAC Address	
HR-MS2Addr	48	MAC Address	
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
Encrypted DMK	1024	Public key encryption using HR-MS1's Public key	
SigHR-MS2	1024	Signature of message generated by using its RSA private key	
HR-MS2_Certific	1024	RSA Digital certificate	

ate			
}			
If(Key Agreement Type == 2) {			
Timestamp_HR-BS	32	Timestamp	
NONCE_HR-BS	64	A random number of 64 bits used for freshness	
HR-BSdAddr	48	MAC Address	
HR-BSAddr	48	MAC Address	
NONCE_HR-BSd	64	A random number of 64 bits used for freshness	
Encrypted B2MK	1024	Public key encryption using HR-MS1's Public key	
SigHR-BS	1024	Signature of message generated by using its RSA private key	
HR-BS_Certificate	1024	RSA Digital certificate	
}}			

Table 18: Modified Table 727 -AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Condition
PKM v3 message type code	4	- PKMv3 EAP-Transfer; PKM v3 message code =2 - PKMv3 Key_Agreement-MSG#1;	

		PKM v3 message code =3 - PKMv3 Key_Agreement-MSG#3; PKM v3 message code =5 - PKMv3 TEK-Reply; PKM v3 message code =7 - PKMv3 TEK-Invalid; PKM v3 message code =8 - Peer_KeyAgreement_MSG #1; PKM v3 message code = 9 - Peer_KeyAgreement_MSG #3; PKM v3 message code = 11 12-16: Reserved	
PKM identifier	8	A value used to match an ABS response to the AMS requests or an AMS response to the ABS requests or an HR-MS response to another HR-MS request	
CMAC indicator	1	Indicates whether this message is protected by CMAC tuple 0: Not protected 1: Protected	Shall always be present
If(PKM v3 message code ==2) {			
EAP payload	variable (1..14 00 x 8)	Contains the EAP authentication data, not interpreted in the MAC	

}			
If(PKM v3 message code == 3) {			
...			
...			
}			
If(PKM v3 message code == 8) {			
SAID	8	Security association identifier	
}			
If(PKM v3 message code == 9) {			
Key Agreement Type	8	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI 2: BS-to-BS security 3-255: Reserved	
If(Key Agreement Type == 0) {			
NONCE_HR-	64	A random number of 64 bits	

MS1		used for freshness	
DAKID	64	identifies the direct communications authorization key	
Key_lifetime	32	DMK key lifetime	
}			
If(Key Agreement Type == 1) {			
Timestamp_HR-MS1	32	Timestamp	
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
HR-MS2Addr	48	MAC Address	
HR-MS1Addr	48	MAC Address	
SigHR-MS1	1024	Signature of message generated by using its RSA private key	
HR-MS1_Certificate	1024	RSA Digital certificate	
}			
If(Key Agreement Type == 2) {			
Timestamp_HR-BSd	32	Timestamp	
NONCE_HR-BSd	64	A random number of 64 bits used for freshness	

HR-BSAddr	48	MAC Address	
HR-BSdAddr	48	MAC Address	
SigHR-BSd	1024	Signature of message generated by using its RSA private key	
HR-BSd_Certificate	1024	RSA Digital certificate	
}}			
If(PKM v3 message code == 11) {			
Key Agreement Type indicator	8	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI 2: BS-to-BS security 3-255: Reserved	
If(Key Agreement Type indicator == 0) {			
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
size of	1	0: size of ICV = 32 bits	

ICV		(default; Max Invalid value is 4096) 1: size of ICV = 64 bits (Max Invalid value is not used)	
PN window Size	16	The receiver shall track PNs within this window to prevent replay attacks	
}			
If (Key Agreement Type indicator == 1) {			
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
HR-MS2Addr	48	MAC Address	
HR-MS1Addr	48	MAC Address	
}			
If (Key Agreement Type indicator == 2) {			
NONCE_HR-BS	64	A random number of 64 bits used for freshness	
HR-BSAddr	48	MAC Address	
HR-BSdAddr	48	MAC Address	
}}			

In the following, the amendments of the Privacy Key Management (PKM) messages in IEEE P802.16n (802.16rev3 baseline) according to one embodiment to support a security procedure for direct communication data security are described.

The Privacy Key Management (PKM) messages are located in Section 6.3.2.3.9 of the 802.16e standards. The modified Table 50 –PKM message codes according to one embodiment are as follows:

Table 19: Modified Table 50 –PKM message codes

Code	PKM message type	MAC management message name
0-2	<i>Reserved</i>	–
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
...	...	...
...	...	...
33	MIH Comeback Response	PKM-RSP
34	DirectComms_KeyAgreement_MSG #1	PKM-RSP
35	DirectComms_KeyAgreement_MSG #2	PKM-REQ
36	DirectComms_KeyAgreement_MSG #3	PKM-RSP
37	PKIDirectComms_KeyAgreement_M SG #1	PKM-RSP
38	PKIDirectComms_KeyAgreement_M SG #2	PKM-REQ
39	PKIDirectComms_KeyAgreement_M	PKM-RSP

	SG #3	
40- 255	Reserved	-

According to one embodiment, a procedure for establishing secure communications between HR-BS in IEEE 802.16n which deals with BS-to-BS security is provided. According to this
5 embodiment, a secure forwarding of data between HR-infrastructure stations is performed using a Public Key Infrastructure (PKI).

This procedure provides strong protection and data integrity
10 when data is forwarded between HR-infrastructure stations (e.g. HR-BS) using a Public Key Infrastructure. Each HR-BS has a public/private key pair and digital certificate (e.g. X.509) issued by a certification authority for mutual authentication and key exchange prior to the start of this
15 direct communications.

The key agreement handshake procedure described below with reference to figures 13 and 14 is for example used for HR-BSs to mutually authenticate themselves (without access to a
20 security server) using PKI and to derive data security keys for secure direct communications. A control connection between the HR-BSs via a designated forwarding HR-MS shall be used for transmitting the key agreement messages.

25 Figure 13 shows a message flow diagram 1300 according to an embodiment.

The message flow takes place between a first base station 1301 which is in this example a degraded HR-BS and is
30 referred to as HR-BSd and a second base station 1302 which is

referred to as HR-BS.

The various steps of the procedure are described in more detail in figure 14.

5

Figure 14 shows a flow diagram 1400 according to an embodiment.

The key agreement handshake procedure using Public Key Infrastructure according to this embodiment includes the following steps 1401 to 1404:

Step 1401: Prior to secure connection establishment, the degraded HR-BS (HR-BSd) 1301 generates a nonce NONCE_HR-BSd .
15 In 1303, the HR-BSd 1301 computes the signature $\text{SigHR-BSd} = \text{SIGN}(\text{Timestamp_HR-BSd} | \text{NONCE_HR-BSd} | \text{HR-BS MAC Addr} | \text{HR-BSd MAC Addr})$ and sends, in 1304, a $\text{BStoBS_KeyAgreement_MSG_}\#1$ message 1305 to the Designated HR-BS 1302, where
 $\text{BStoBS_KeyAgreement_MSG_}\#1 = \text{Timestamp_HR-BSd} | \text{NONCE_HR-BSd} | \text{HR-BS MAC Addr} | \text{HR-BSd MAC Addr} | \text{SigHR-BSd} | \text{HR-BSd_Certificate}$.
20

Step 1402: The HR-BS 1302 first verifies the received timestamp and nonce for freshness and the certificate HR-BSd_Certificate and signature SigHR-BSd in 1306. If the verifications fail, then the HR-BS 1302 ignores the $\text{BStoBS_KeyAgreement_MSG_}\#1$ message. If the verifications are correct, then the HR-BS 1302, in 1307, generates a nonce NONCE_HR-BS and security key B2MK and computes $\text{B2AK} = \text{Dot16KDF}(\text{B2MK}, \text{HR-BSd MAC Addr} | \text{HR-BS MAC Addr} | \text{"B2AK"}, 160)$ and the B2CMAC key and $\text{CMAC_HR-BS} = \text{MAC}_{\text{B2CMAC}}(\text{NONCE_HR-BS} | \text{NONCE_HR-BSd} | \text{HR-BS MAC Addr} | \text{HR-BSd MAC Addr})$. The HR-BS 1302 then uses the HR-BSd's 1301 public key to encrypt and obtain Encrypted
25
30

B2MK = $E_{HR-BSd_PK}(B2MK, key_lifetime, HR-BSd\ MAC\ Addr, HR-BS\ MAC\ Addr)$. Finally, in 1308, the HR-BS 1301 computes signature $Sig_{HR-BS} = SIGN(T_{HR-BS} | NONCE_{HR-BS} | HR-BSd\ MAC\ Addr | HR-BS\ MAC\ Addr | NONCE_{HR-BSd} | Encrypted\ B2MK | CMAC_{HR-BS})$ and sends, in
 5 1309, a BStoBS_KeyAgreement_MSG_#2 message 1310 to HR-BSd, where $BStoBS_KeyAgreement_MSG_#2 = T_{HR-BS} | NONCE_{HR-BS} | HR-BSd\ MAC\ Addr | HR-BS\ MAC\ Addr | NONCE_{HR-BSd} | Encrypted\ B2MK | CMAC_{HR-BS} | Sig_{HR-BS} | HR-BS_Certificate$.

10 Step 1403: The HR-BSd 1301 in 1311 first verifies the received timestamp and nonces for freshness and the certificate $HR-BS_Certificate$ and signature $signature_{HR-BS}$. If the verification is invalid, then HR-BSd ignores the BStoBS_KeyAgreement_MSG_#2 message 1310. If the verifications
 15 are correct, then the HR-BSd 1301 in 1312 decrypts Encrypted B2MK and obtains security key B2MK and $key_lifetime$. Next, HR-BSd 1301 computes B2AK and B2CMAC keys and verifies $CMAC_{HR-BS}$ in 1313. If the verification is invalid, then HR-BSd ignores the BStoBS_KeyAgreement_MSG_#2 message 1310. If
 20 the verification is correct, then HR-BSd computes $CMAC_{HR-BSd} = MAC_{B2CMAC}(NONCE_{HR-BSd} | NONCE_{HR-BS} | HR-BSd\ MAC\ Addr | HR-BS\ MAC\ Addr)$ and sends, in 1314, a BStoBS_KeyAgreement_MSG_#3 message 1315 to the HR-BS 1302, where
 $BStoBS_KeyAgreement_MSG_#3 = NONCE_{HR-BS} | HR-BS\ MAC\ Addr | HR-BSd\ MAC\ Addr | CMAC_{HR-BSd}$. If the HR-BSd 1301 does not receive BStoBS_KeyAgreement_MSG_#2 message 1310 from the HR-BS 1302
 25 within BStoBS_KeyAgreement_MSG_#1 Timeout, it resends the BStoBS_KeyAgreement_MSG_#1 message 1305 up to BStoBS_KeyAgreement_MSG_#1 MaxResends times. If HR-BSd 1301
 30 reaches its maximum number of resends, it initiates another authentication or drop the request.

Step 1404: The HR-BS 1302 receives the

BStoBS_KeyAgreement_MSG_#3 message 1315 and in 1316 verifies the received nonce and the CMAC tuple. If the verification fails, then HR-BS ignores BStoBS_KeyAgreement_MSG_#3 message 1315. If the verification is correct, then the HR-BS 1302 confirms that HR-BSd 1301 has computed the correct keys and commences secure direct communications. If the HR-BS 1302 does not receive the BStoBS_KeyAgreement_MSG_#3 message 1414 from the HR-BSd 1301 within BStoBS_KeyAgreement_MSG_#2 Timeout, it shall resend the BStoBS_KeyAgreement_MSG_#2 message up to BStoBS_KeyAgreement_MSG_#2 MaxResends times. If the HR-BS 1302 reaches its maximum number of resends, it shall initiate another authentication or drop the request. The HR-BSd 1301 and the HR-BS 1302 can now, in 1317 and 1318, derive B2TEK and commence secure connection establishment.

The messages 1305, 1310 and 1315 are in one embodiment for example formed according to the following tables 20 to 23.

Table 20: Secure forwarding between HR-infrastructure stations using Public Key Infrastructure message type

Code	Key Agreement Type	Message Type	MAC control message name
9	2	Peer_KeyAgreement_MSG #1	AAI-PKM-RSP
10	2	Peer_KeyAgreement_MSG #2	AAI-PKM-REQ
11	2	Peer_KeyAgreement_MSG #3	AAI-PKM-RSP

Table 21: Peer_KeyAgreement_MSG_#1 message attribute

Attribute	Contents
Timestamp_HR-BSd	Timestamp generated by HR-BSd
NONCE_HR-BSd	Freshly generated random number of 64bits by HR-BSd
HR-BS MAC Addr	MAC Address of HR-BS
HR-BSd MAC Addr	MAC Address of HR-BSd
SigHR-BSd	Signature of message generated by HR-BSd using its RSA private key
HR-BSd_Certificate	Digital certificate of HR-BSd

Table 22: Peer_KeyAgreement_MSG_#2 message attribute

Attribute	Contents
Timestamp_HR-BS	Timestamp generated by HR-BS
NONCE_HR-BS	Freshly generated random number of 64bits by HR-BS
HR-BSd MAC Addr	MAC Address of HR-BSd
HR-BS MAC Addr	MAC Address of HR-BS
NONCE_HR-BSd	Nonce generated by HR-BSd in BStoBS_KeyAgreement_MSG_#1 message
Encrypted B2MK	Public key encryption $E_{HR-BSd_PK}(B2MK, key_lifetime, HR-BSd\ MAC\ Addr, HR-BS\ MAC\ Addr)$ using HR-BSd's Public key where $B2MK = BStoBS$ Master Key generated by HR-MS and $key_lifetime = lifetime\ of\ B2MK$
CMAC_HR-BS	Message digest calculated using B2CMAC key by HR-BS

SigHR-BS	Signature of message generated by HR-BS using its RSA private key
HR-BS_Certificate.	Digital certificate of HR-BS

Table 23: Peer_KeyAgreement_MSG_#3 message attribute

Attribute	Contents
NONCE_HR-BS	Nonce generated by HR-BS in BStoBS_KeyAgreement_MSG_#2 message
HR-BS MAC Addr	MAC Address of HR-BS
HR-BSd MAC Addr	MAC Address of HR-BSd
CMAC_HR-BSd	Message digest calculated using B2CMAC key by HR-BSd

5

In the following a BS to BS communications security context according to one embodiment is described that describes the set of parameters that links the BS to BS security keys for secure forwarding between HR-infrastructure stations.

10

The B2MK context includes all parameters associate with the B2MK. This context is created when the B2MK is derived.

The B2MK context according to one embodiment is described in Table 24.

15

Table 24: The B2MK context

Parameter	Size (bit)	Usage
-----------	-------------------	-------

B2MK	160	BS-to-BS Master Key shared by HR-BS and HR-BSd
B2MK SN	4	B2MK sequence number
B2MK Lifetime	32	B2MK Lifetime
B2AK_COUNT	16	Counter to ensure freshness of computed CMAC key and prevent replay attacks.

The B2AK context includes all parameters associate with the B2AK. This context is created whenever a new B2AK is derived. According to one embodiment, this context is deleted when the

5 B2AK is not in used.

The B2AK context according to one embodiment is described in Table 25.

10

Table 25: The B2AK context

Parameter	Size (bit)	Usage
B2AK	160	BS-to-BS Communications Authentication Key derived from B2MK.
B2AK Lifetime	32	B2AK Lifetime
B2AKID	64	Identifies the B2AK key.
B2CMAC_KEY	128	Key which is used for signing BS-to-BS Communications MAC control messages.
B2CMAC_PN	24	Used to avoid BS-to-BS communication replay attack on the control connection. The initial value of B2CMAC_PN is zero.

B2AK_COUNT	16	Counter to ensure freshness of computed B2CMAC key and prevent replay attacks.
------------	----	--

The B2SA context is the set of parameters managed by each B2SA in order to ensure B2TEK management and usage in a secure way for secure forwarding between HR-infrastructure stations.

The B2SA holds the B2TEK context and additional information that belongs to the B2SA itself.

10 The B2TEK context includes all parameters of the B2TEK. The B2TEK context according to one embodiment is described in Table 26.

15 Table 26: The B2TEK context

Parameter	Size (bit)	Usage
B2TEK	128	Key used for encryption or decryption of BS-to-BS communications messages
B2MK SN	4	B2MK sequence number
COUNTER_B2TEK	16	The counter used to derive this B2TEK
B2TEK lifetime	32	B2TEK lifetime=B2MK lifetime
B2TEK_PN	22	The PN used for encrypting BS-to-BS communication packets. After each BS-to-BS communication MAC PDU transmission, the value shall be increased by 1. (0x000000-0x1FFFFFF)

The B2SA context according to one embodiment is described in Table 27.

5

Table 27: The B2SA context

Parameter	Size (bit)	Usage
B2SAID	8	The identifier of this B2SA, which describes the applied encryption/decryption method and B2TEK contexts.
B2TEK context	Size of (B2TEK context)	B2TEK context for encryption and decryption

In the following, the key derivation for secure forwarding
10 between HR-infrastructure stations using a Public Key
Infrastructure according to one embodiment is described.

The key hierarchy defines what keys are present in the system
for secure forwarding between HR-infrastructure stations and
15 how the keys are generated.

The B2MK is the security key that is randomly generated by
HR-BS. The B2MK is a 160-bit key.

20 The B2MK may be used as a source for keying materials
required by upper layers.

The B2MK is used to derive the BS-to-BS Communication Authentication Key (B2AK).

5 B2AK is derived from B2MK and belongs to a pair of HR-BSs (HR-BSd and HR-BS). The B2AK is used for secure forwarding between HR-infrastructure stations.

According to one embodiment, the B2AK derivation is as follows:

10
$$\text{B2AK} = \text{Dot16KDF}(\text{B2MK}, \text{HR-BSd MAC Addr} \parallel \text{HR-BS MAC Addr} \parallel \text{"B2AK"}, 160)$$

where: HR-BSd MAC Addr and HR-BS MAC Addr are the addresses of HR-BSd and HR-BS respectively.

15 The B2CMAC-B2TEK prekey is derived from B2AK and is used to derive other keys:

- BS-to-BS Communication Cipher-based Message Authentication Code (B2CMAC) key
- BS-to-BS Communication Traffic Encryption (B2TEK) Key

20

According to one embodiment, the B2CMAC-B2TEK prekey derivation is done as follows:

$$\text{B2CMAC-B2TEK prekey} = \text{Dot16KDF}(\text{B2AK}, \text{B2AK_COUNT} \parallel \text{"B2CMAC-B2TEK prekey"}, 160)$$

25

The B2CMAC key is derived from B2AK and used for message authentication for the messages sent during secure forwarding between HR-infrastructure stations.

According to one embodiment, the B2CMAC key is derived as follows:

30

$$\text{B2CMAC key} = \text{Dot16KDF}(\text{B2CMAC-B2TEK prekey}, \text{"B2CMAC_KEYS"}, 128)$$

B2TEK is the transport encryption key used to encrypt data in secure forwarding between HR-infrastructure stations.

According to one embodiment, the B2TEK is derived as follows:

$$\text{B2TEK} = \text{Dot16KDF}(\text{B2CMAC-B2TEK prekey},$$

5 $\text{B2SAID}|\text{COUNTER_B2TEK}|"B2TEK_KEY", 128)$

where B2SAID is the security association to which the B2TEK belongs.

COUNTER_B2TEK is a counter used to derive different B2TEKs
10 for the same B2SAID, the value of the counter is changed every time a new B2TEK needs to be derived within the same B2AK and B2AK_COUNT pair is valid. Every time a new B2CMAC-B2TEK prekey is derived, this counter is reset.

15 Another example for a security authorization and key exchange is described in the following with reference to figure 15.

Figure 15 shows a message flow diagram 1500 according to an embodiment.

20

The message flow takes place between a first mobile terminal 1501 for example corresponding to the first mobile terminal 301, a second mobile terminal 1502 for example corresponding to the second mobile terminal 302 and a base station 1503 for
25 example corresponding to the base station 303.

Once the HR-BS 1503 has detected that security direct communication between the two HR-MSs 1501, 1502 is possible, HR-BS 1503 sends the security key DMK in 1504 and 1505 to the
30 first HR-MS 1501 and the second HR-MS 1502 (which are assumed to have requested direct communication) with a Key-Transfer-MSG#1 message 1506 and a Key-Transfer-MSG#2 message 1507 (e.g. AAI-PKM-RSP messages). Following this, the HR-MSs 1501,

1502 carry out a 3-way Direct Communications Key Agreement process in 1508 to 1517 in which they exchange key agreement messages DirectComms_KeyAgreement_MSG_#1 (AAI-PKM-RSP MAC Control Message) 1518, DirectComms_KeyAgreement_MSG_#2 (AAI-PKM-REQ MAC Control Message) 1519 and DirectComms_KeyAgreement_MSG_#3 (AAI-PKM-RSP MAC Control Message) 1520.

After the 3-way Direct Communications Key Agreement process, both HR-MS1 1501 and HR-MS2 1502 are able to commence secure direct communications and proceed to the Flow Setup phase.

It should be noted that the flow of figure 15 can be seen as a first part including the DMK being sent from the HR-BS 1502 to the HR-MS1 1501 and HR-MS2 1502 and a second part including the pre-shared key method in more detail.

According to various embodiments, as described above, one or more of the following is provided:

- A method for providing mutual authentication for two HR-MSs with the help of HR-BS for direct communications.
- A method for providing secret keys for data security and data authentication for two HR-MSs with the help of HR-BS for direct communications.
- A method for providing mutual authentication for two HR-MS in direct communications without infrastructure using PKI approach.
- A method for providing secret keys for data security and data authentication for two HR-MS in direct

communications without infrastructure using PKI approach.

- A method for providing mutual authentication for two HR-MS in direct communications without infrastructure where one HR-MS converts to HR-BS* (Multimode).
- A method for providing secret keys for data security and data authentication for two HR-MS in direct communications without infrastructure where one HR-MS converts to HR-BS* (Multimode).
- A method for providing mutual authentication for two HR-MS in direct communications without infrastructure where a pre-shared secret key has been earlier established.
- A method for providing secret keys for data security and data authentication for two HR-MS in direct communications without infrastructure where a pre-shared secret key has been earlier established.
- A method for deriving the DAK and DCMAC keys.

According to various embodiments, authentication and key exchange (AKE) protocols for mutual authentication and data security for IEEE 802.16n HR networks in both network aided and autonomous scenarios are proposed. Specifically, a network-aided AKE protocol in which the HR-BS (base station) assists the two HR-MSs to establish a Direct Communication Master Key (DMK) which would be used for data security and mutual authentication for direct communications is described. Further, three different AKE solutions/protocols for autonomous mutual authentication of HR-MSs and data security

for direct communications are described. The first autonomous AKE solution includes a PKI approach, whereby each HR-MS possess a digital certificate which can be used for mutual authentication and key exchange for data security in direct communications between two HR-MSs without backbone network. The second autonomous AKE solution can be used in the event where one HR-MS converts into a Base Station (denoted as HR-BS*) when there is no backbone network (i.e. no HR-BS) in the environment. Finally, the third autonomous AKE solution is used in the event where two HR-MSs that wishes to establish direct communications with each other autonomously have already established a pre-shared key *DMK* using the network-aided AKE protocol described above.

While the invention has been particularly shown and described with reference to specific aspects, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced.

Claims

1. Communication terminal of a cellular mobile
communication system, the cellular mobile communication
5 system comprising the communication terminal, another
communication terminal and a communication network for
providing a communication connection between the
communication terminal and the other communication
terminal via at least one base station of the
10 communication network, the communication terminal
comprising:
a determiner configured to determine an encryption key
for secure communication between the communication
terminal and the other communication terminal via a
15 radio interface between the communication terminal and
the other communication terminal; and
a transceiver configured to perform secure communication
with the other communication terminal via the radio
interface between the communication terminal and the
20 other communication terminal using the determined
encryption key.
2. The communication terminal according to claim 1, wherein
the secure communication is direct communication between
25 the communication terminal and the other communication
terminal.
3. The communication terminal according to claim 2, wherein
the direct communication is communication of data
30 without the data being communicated via a base station
of the communication network.

4. The communication terminal according to any one of claim 2 or 3, wherein the direct communication is communication of data without the communication network being involved in the communication.

5

5. The communication terminal according to any one of claims 1 to 4, wherein the determiner is configured to determine the encryption key by exchanging messages with the other communication terminal via the radio interface between the communication terminal and the other communication terminal.

10

6. The communication terminal according to claim 5, wherein the messages are exchanged via direct communication between the communication terminal and the other communication terminal.

15

7. The communication terminal according to claim 5 or 6, wherein the messages are exchanged between the communication terminal and the other communication terminal without being communicated via a base station of the communication network.

20

8. The communication terminal according to any one of claims 5 to 7, wherein the messages are exchanged between the communication terminal and the other communication terminal without the communication network being involved in the exchange of the messages.

25

9. The communication terminal according to any one of claims 1 to 8, wherein the communication network is a communication network according to a 802.16 communication standard.

30

10. The communication terminal according to any one of
claims 1 to 9, wherein the communication network is a
communication network according to the 802.16n
5 communication standard.
11. The communication terminal according to any one of
claims 1 to 10, wherein the transceiver is configured to
send a request for a direct communication with the other
10 communication terminal to the communication network or
to the other communication terminal.
12. The communication terminal according to claim 11,
wherein the transceiver is configured to include a
15 certificate into the request.
13. The communication terminal according to claim 11 or 12,
wherein the transceiver is configured to include a nonce
into the request.
20
14. The communication terminal according to any one of
claims 1 to 13, wherein the transceiver is configured to
receive the encryption key from the communication
network or from the other communication terminal and
25 wherein the determiner is configured to determine the
encryption key as the received encryption key.
15. The communication terminal according to claim 14,
wherein the transceiver is configured to receive the
30 encryption key with a message from the communication
network or the other communication terminal and is
configured to authenticate the message.

16. The communication terminal according to claim 14 or 15, wherein the transceiver is configured to check the message for message freshness.

5 17. The communication terminal according to any one of claims 1 to 16, wherein the transceiver is configured to send a message including the determined encryption key to the communication network or to the other communication terminal.

10

18. The communication terminal according to claim 17, wherein the transceiver is configured to include a certificate into the request.

15 19. The communication terminal according to claim 17 or 18, wherein the transceiver is configured to include a nonce into the request.

20 20. The communication terminal according to any one of claims 1 to 19, wherein the communication terminal is configured to act as a base station of the communication network.

25 21. The communication terminal according to any one of claims 1 to 20, wherein the determiner is configured to determine the encryption key based on a pre-shared encryption key which was pre-shared between the communication terminal and the other communication terminal.

30

22. A method for performing communication between a communication terminal of a cellular mobile communication system and another communication terminal

of the cellular mobile communication system, the cellular mobile communication system comprising the communication terminal, the other communication terminal and a communication network for providing a communication connection between the communication terminal and the other communication terminal via at least one base station of the communication network, the method comprising:

determining an encryption key for secure communication between the communication terminal and the other communication terminal via a radio interface between the communication terminal and the other communication terminal; and

performing secure communication between the communication terminal and the other communication terminal via the radio interface between the communication terminal and the other communication terminal using the determined encryption key.

100

FIG 1

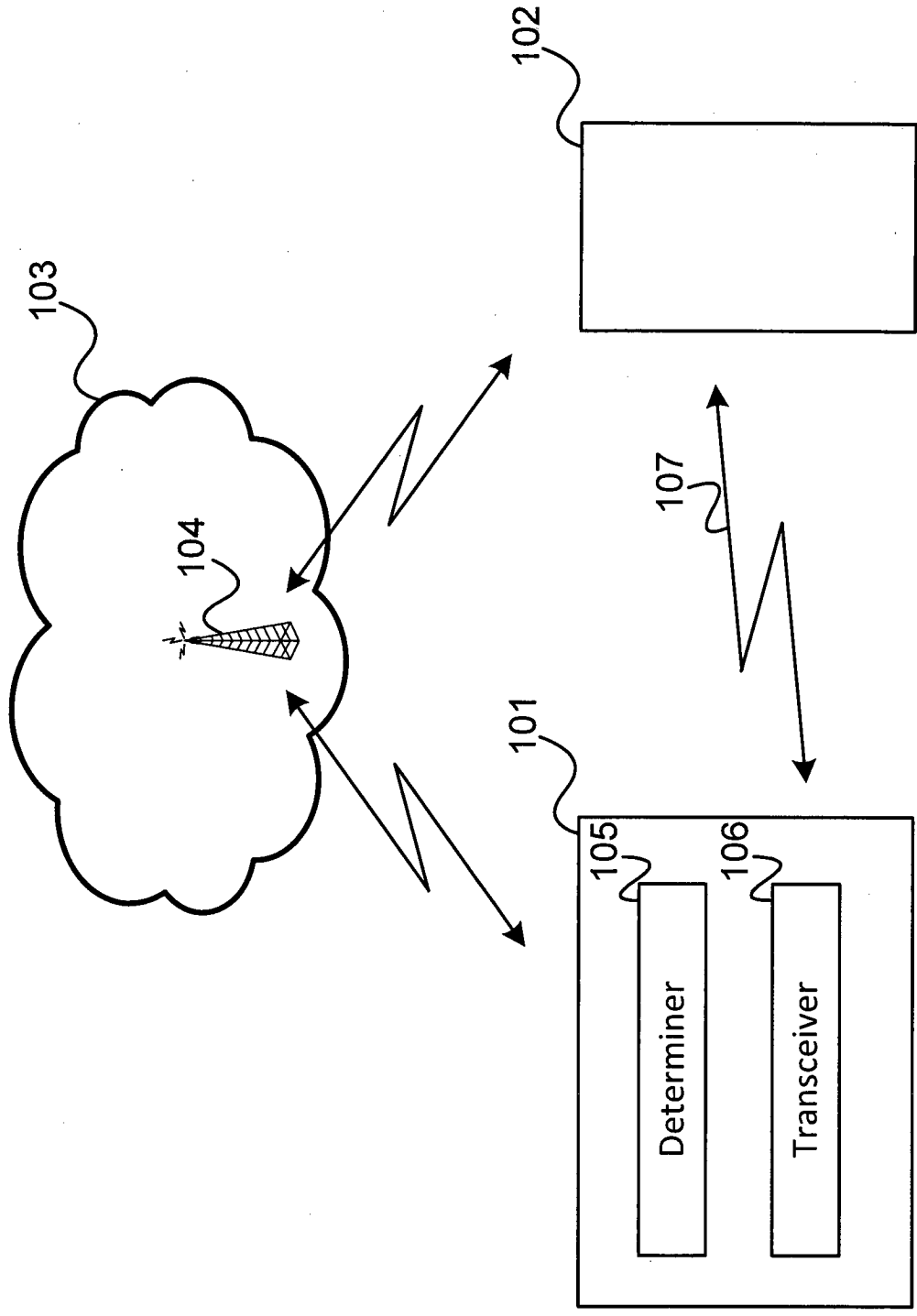


FIG 2

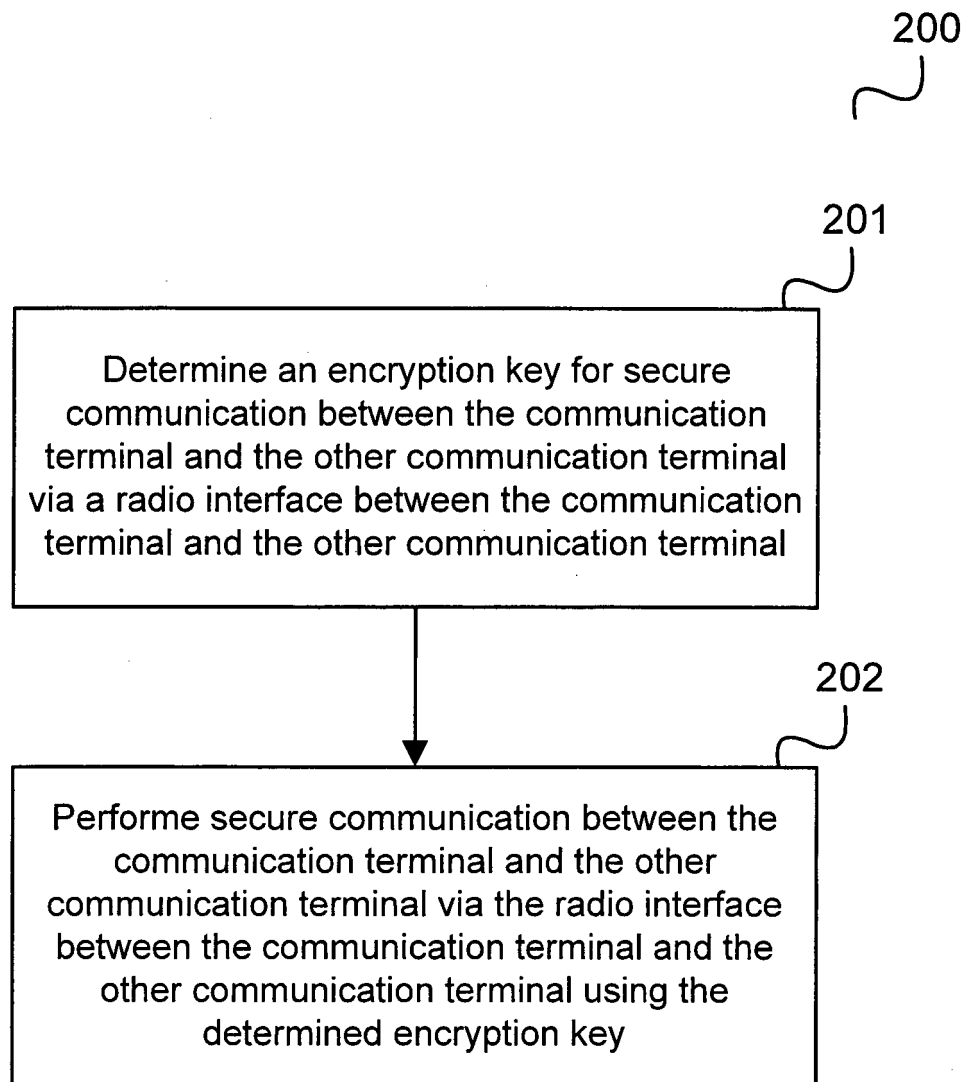
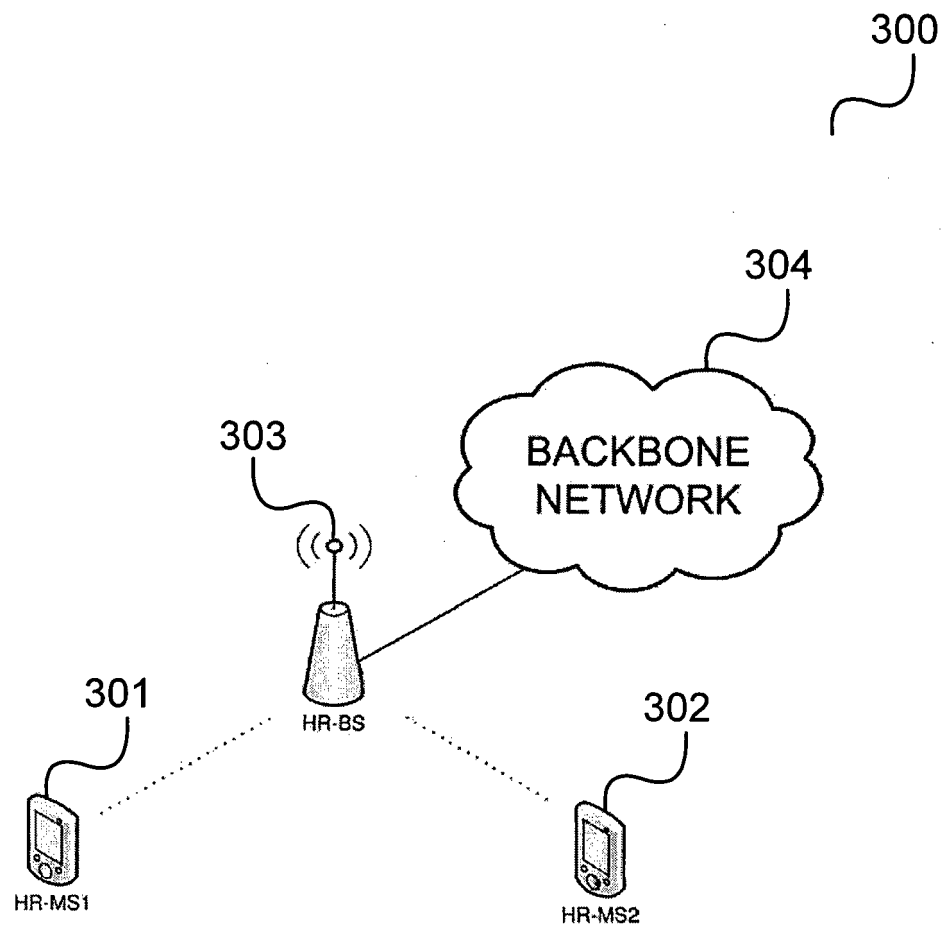


FIG 3



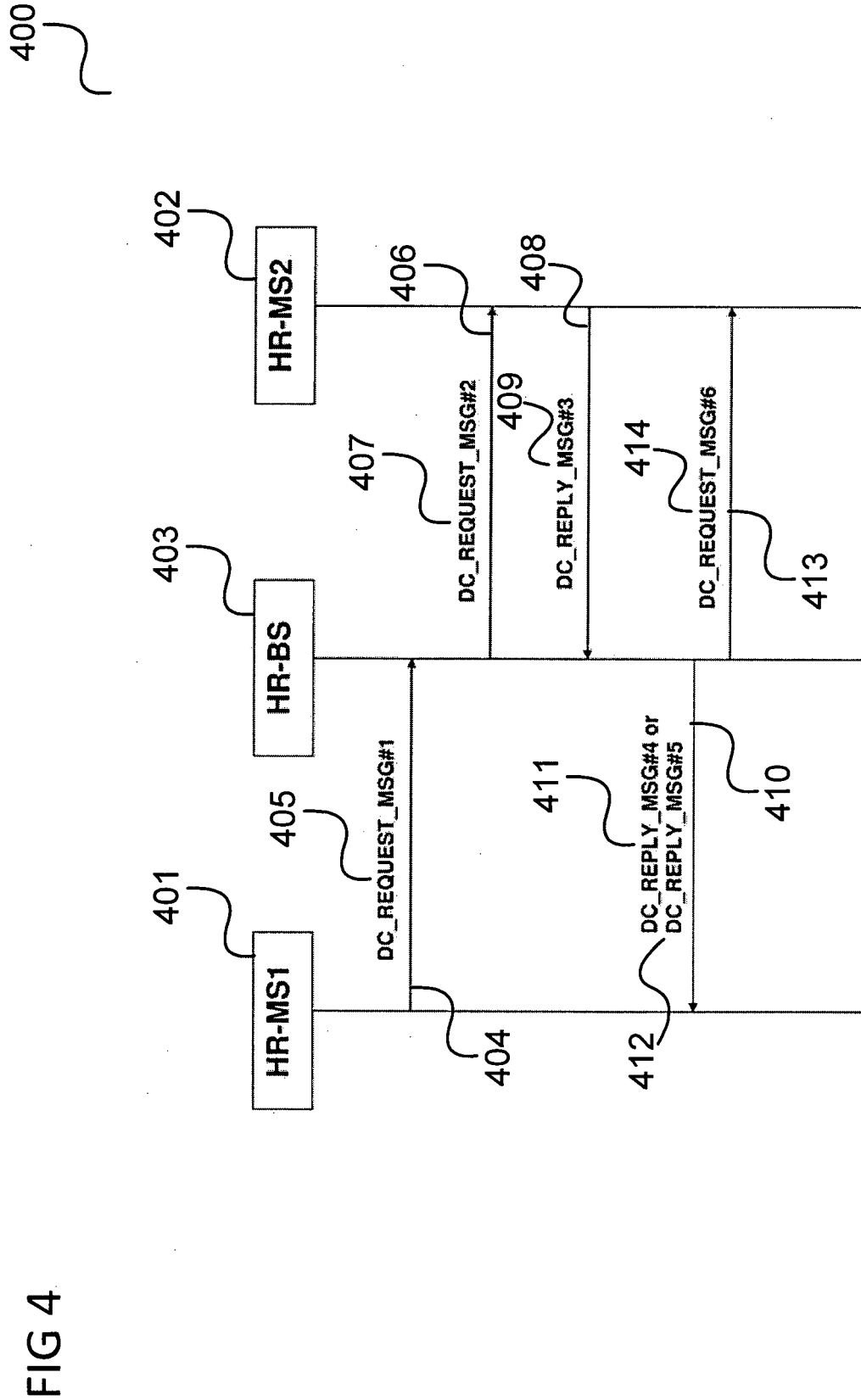


FIG 5

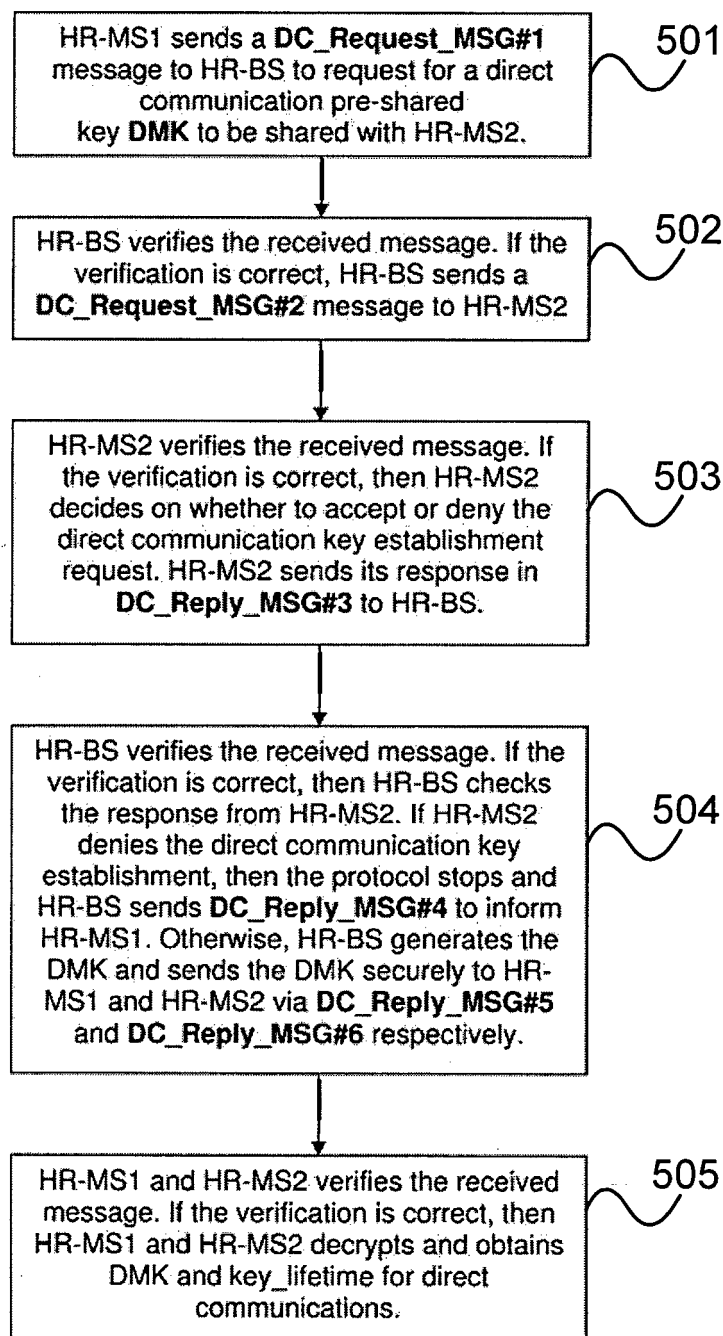


FIG 6

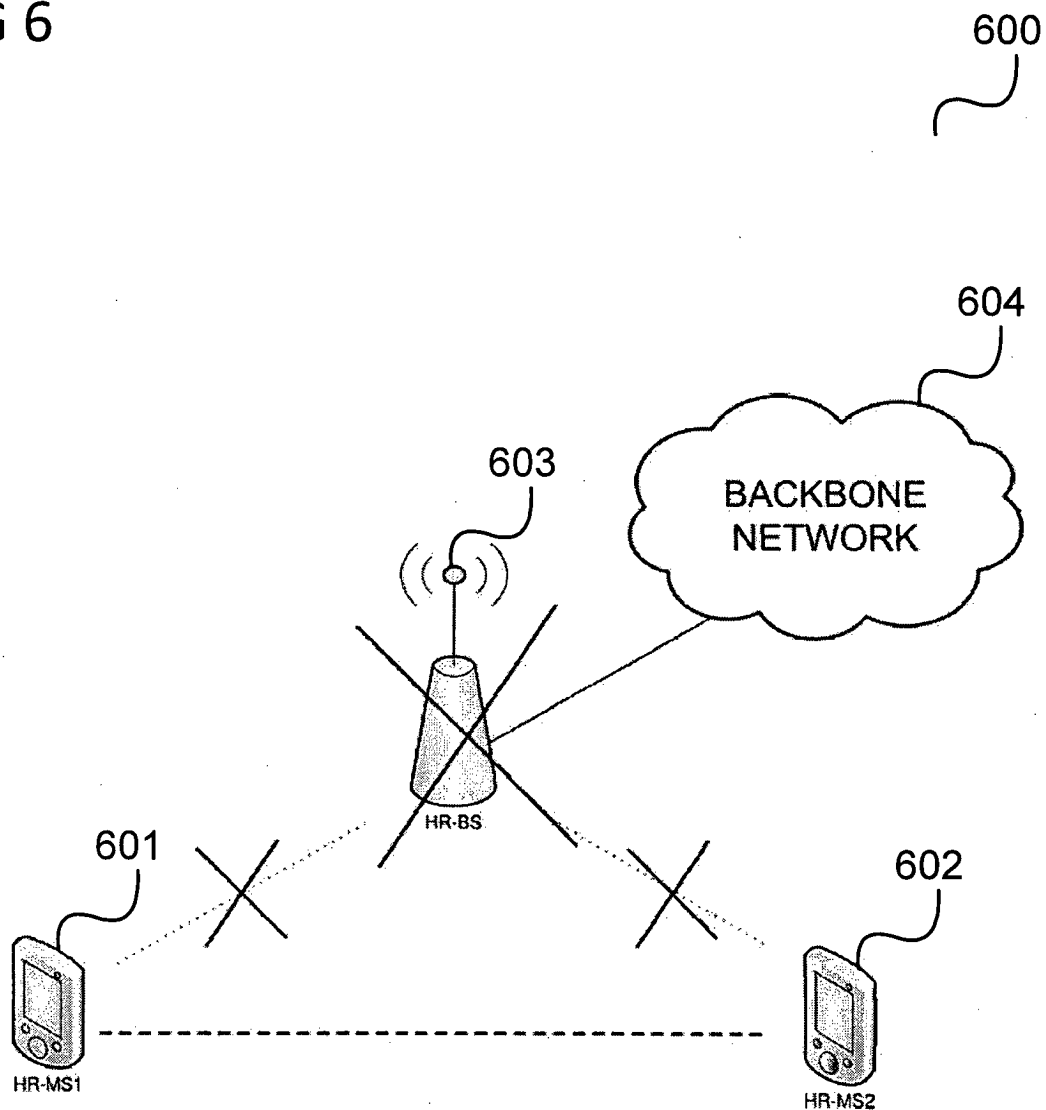


FIG 7

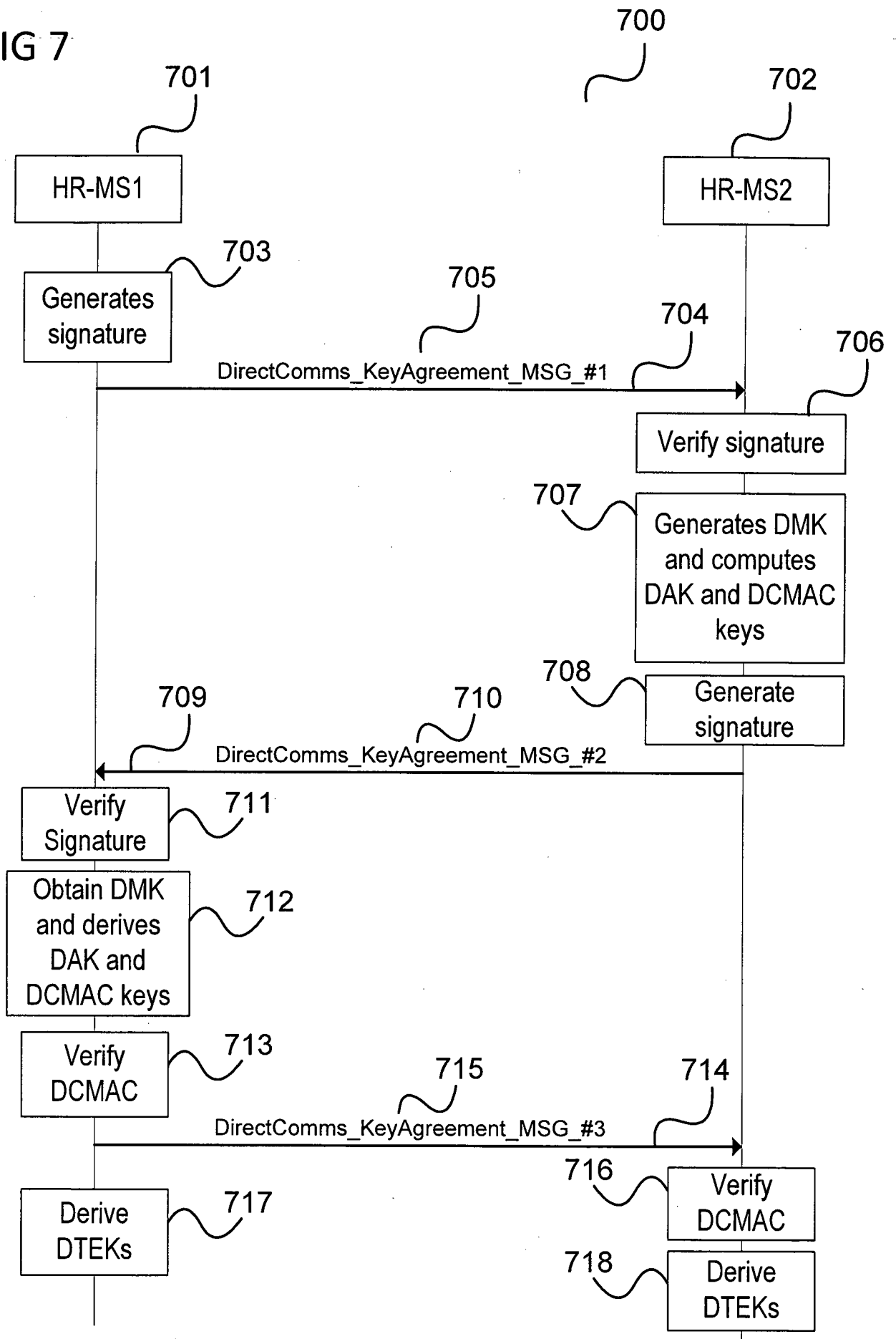


FIG 8

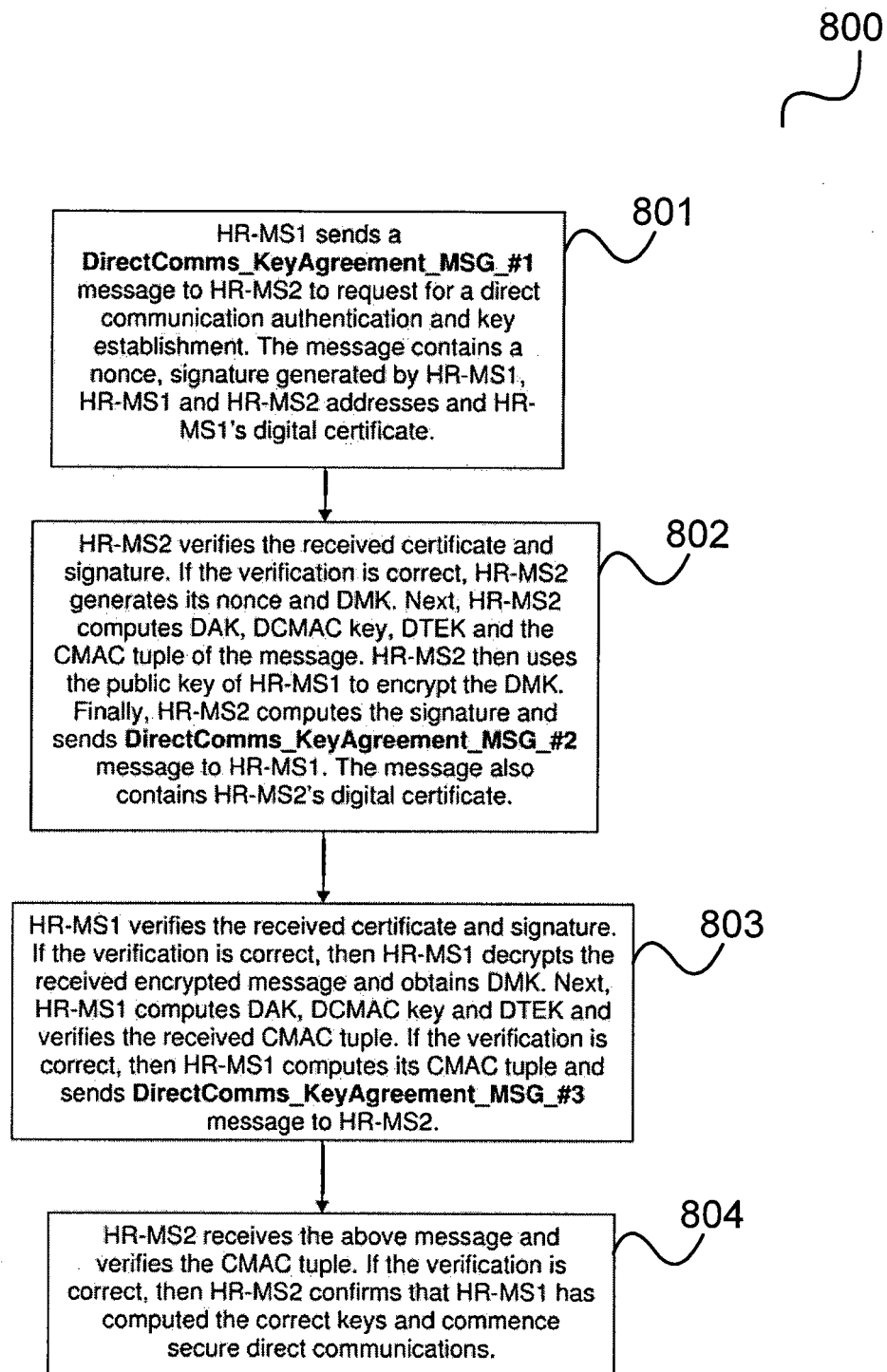


FIG 9

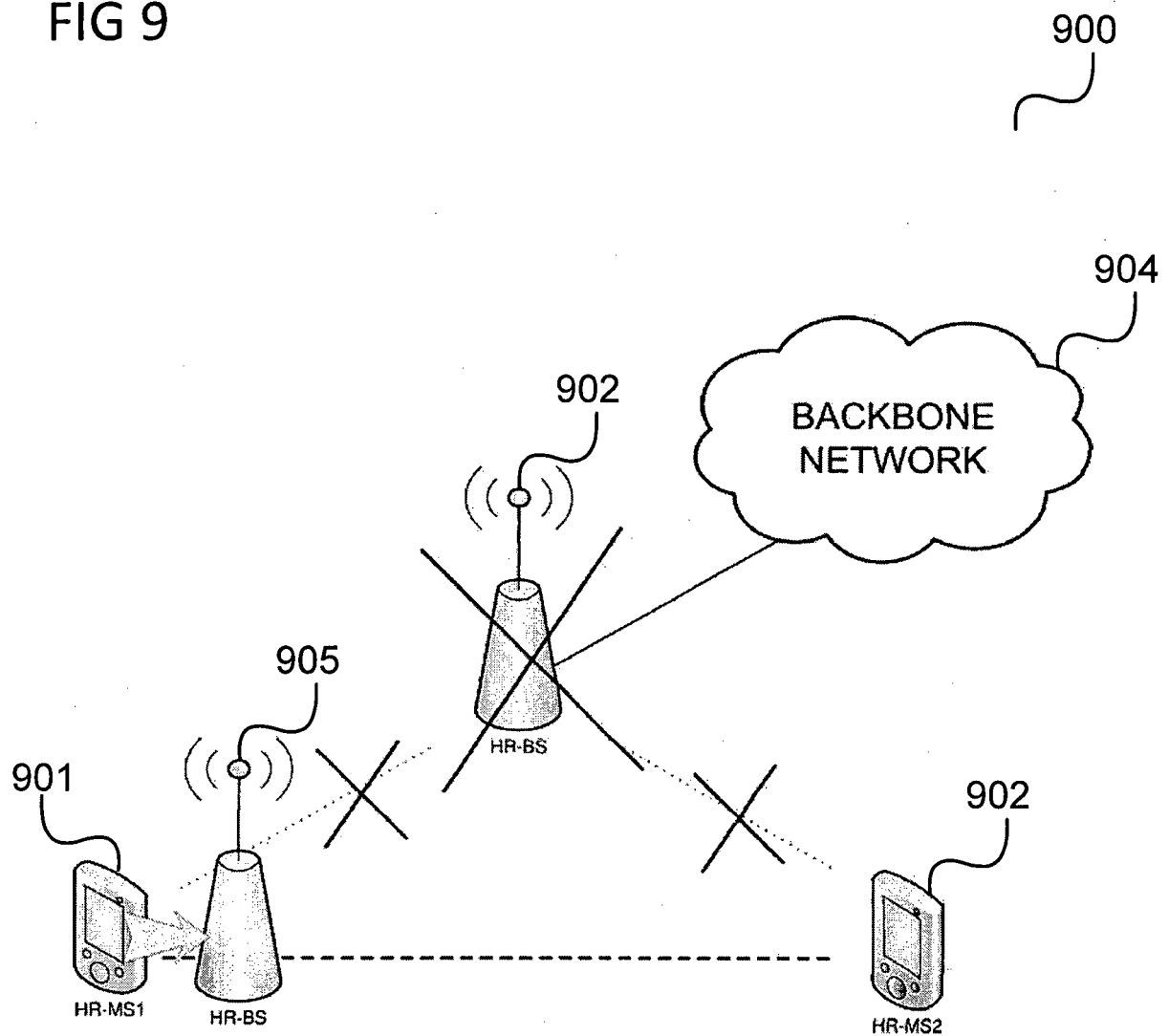


FIG 10

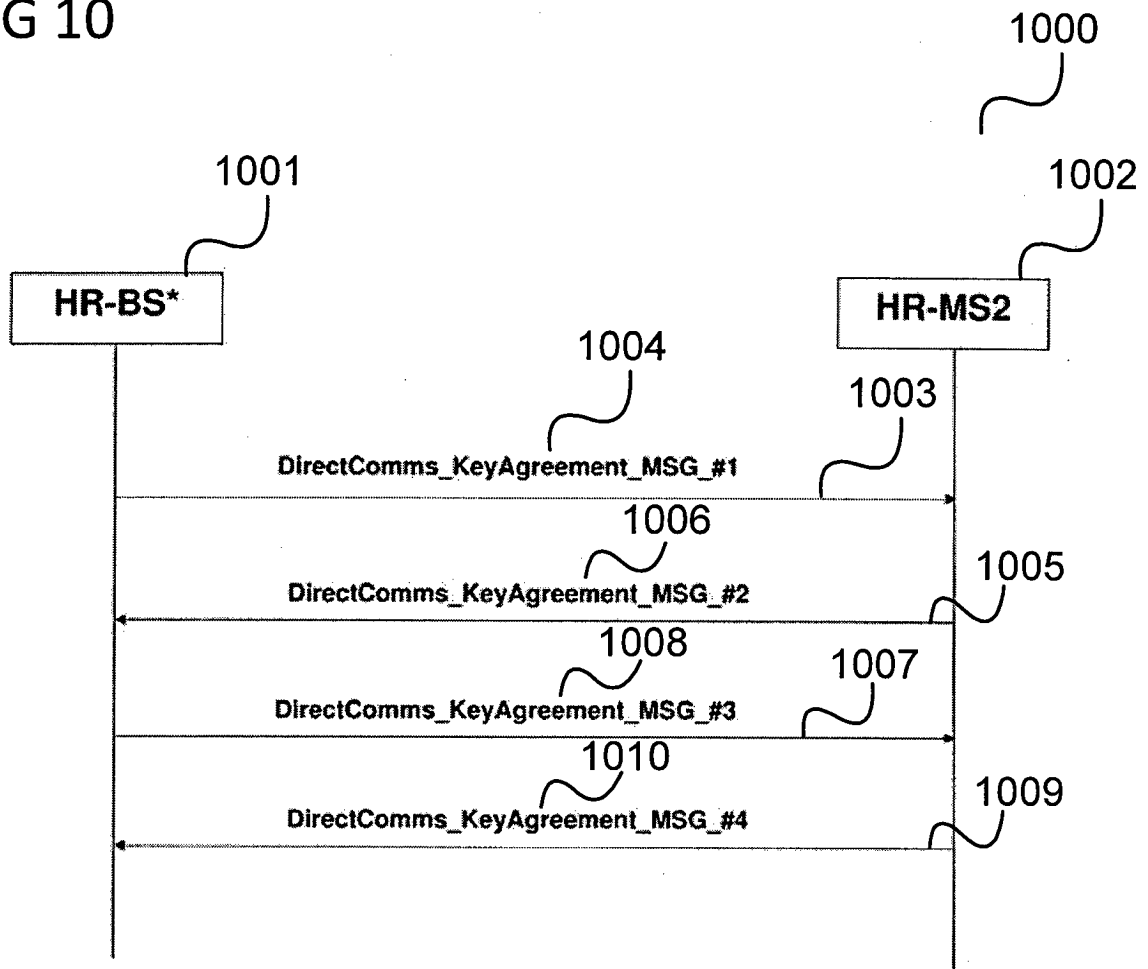


FIG 11

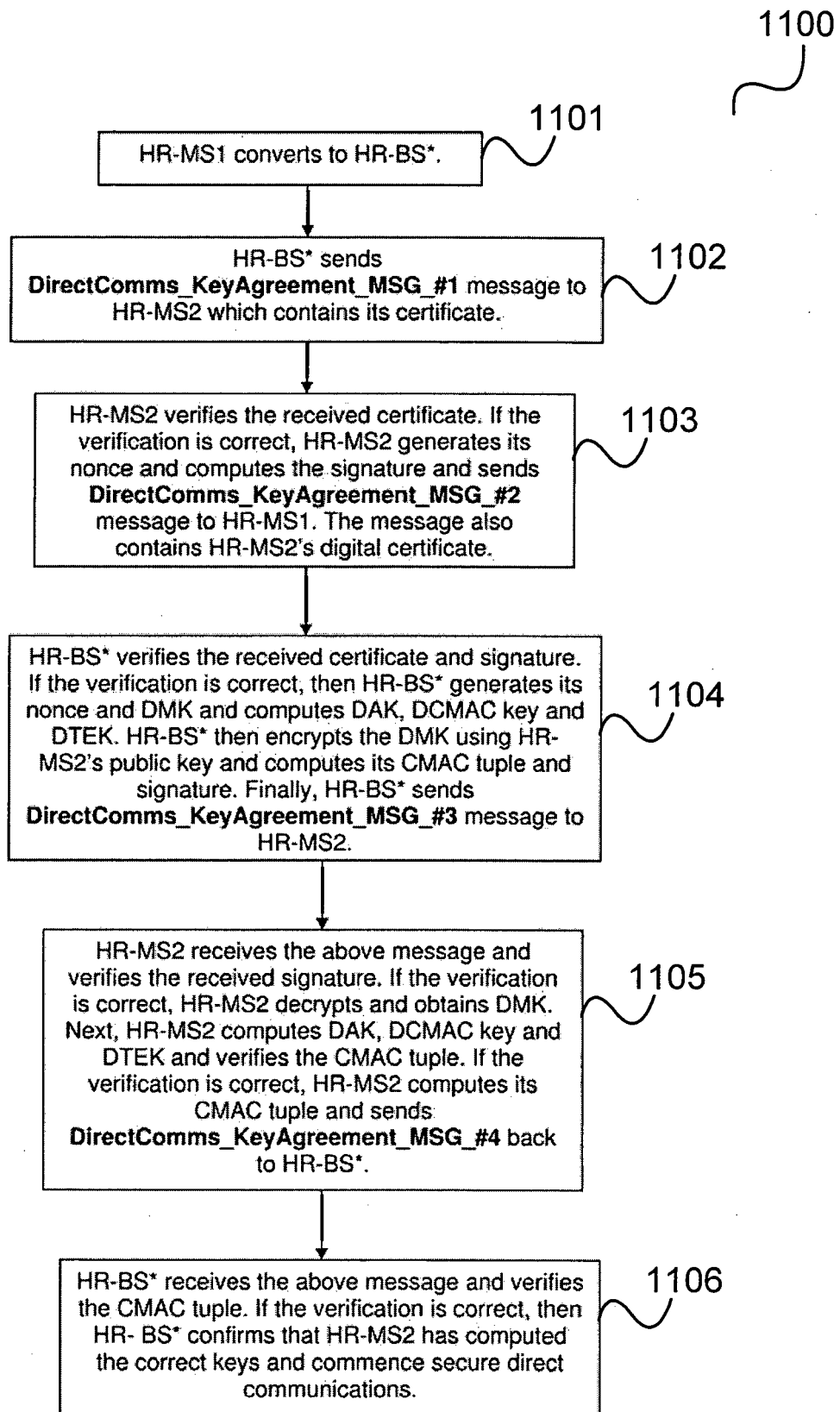


FIG 12

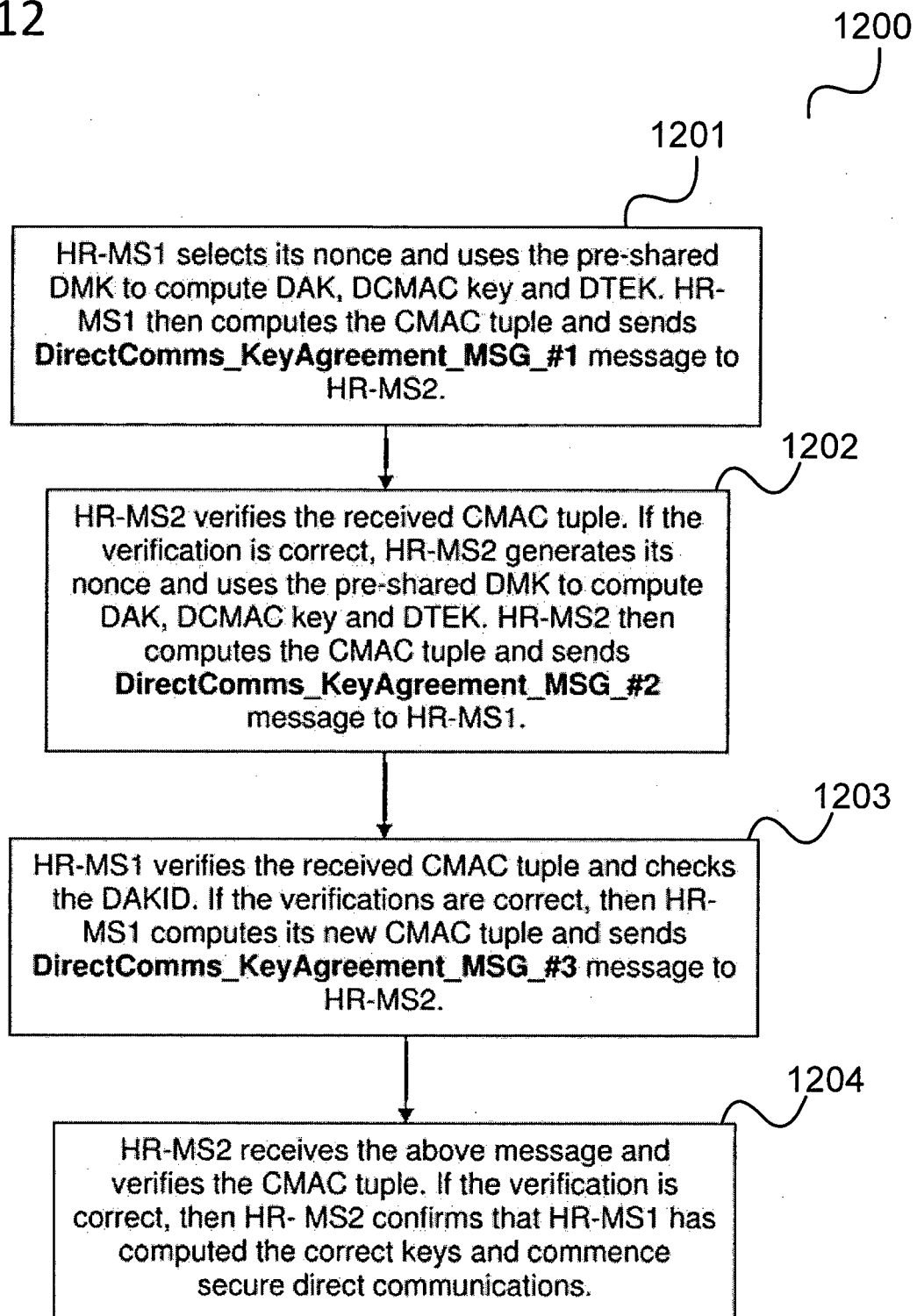


FIG 13

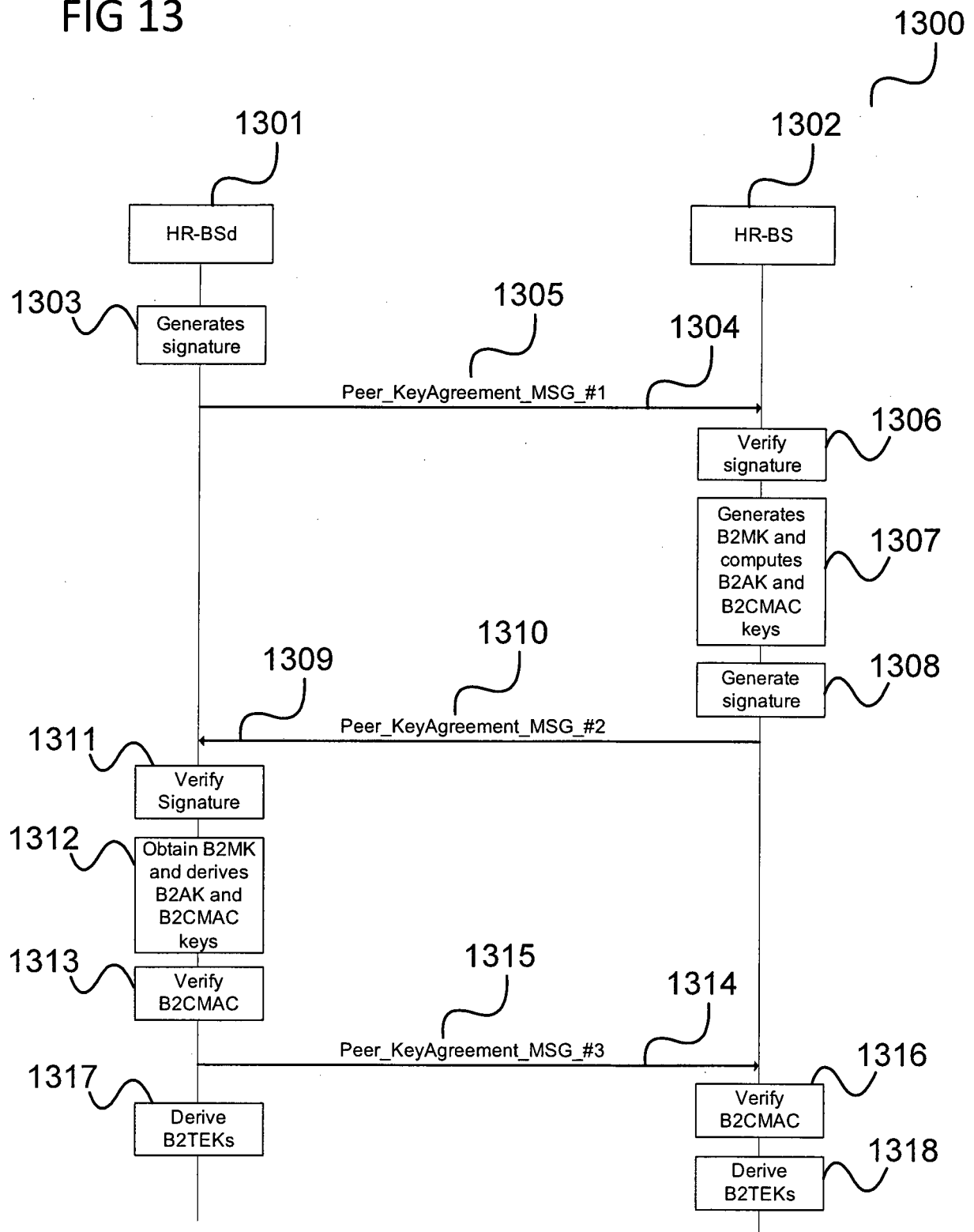


FIG 14

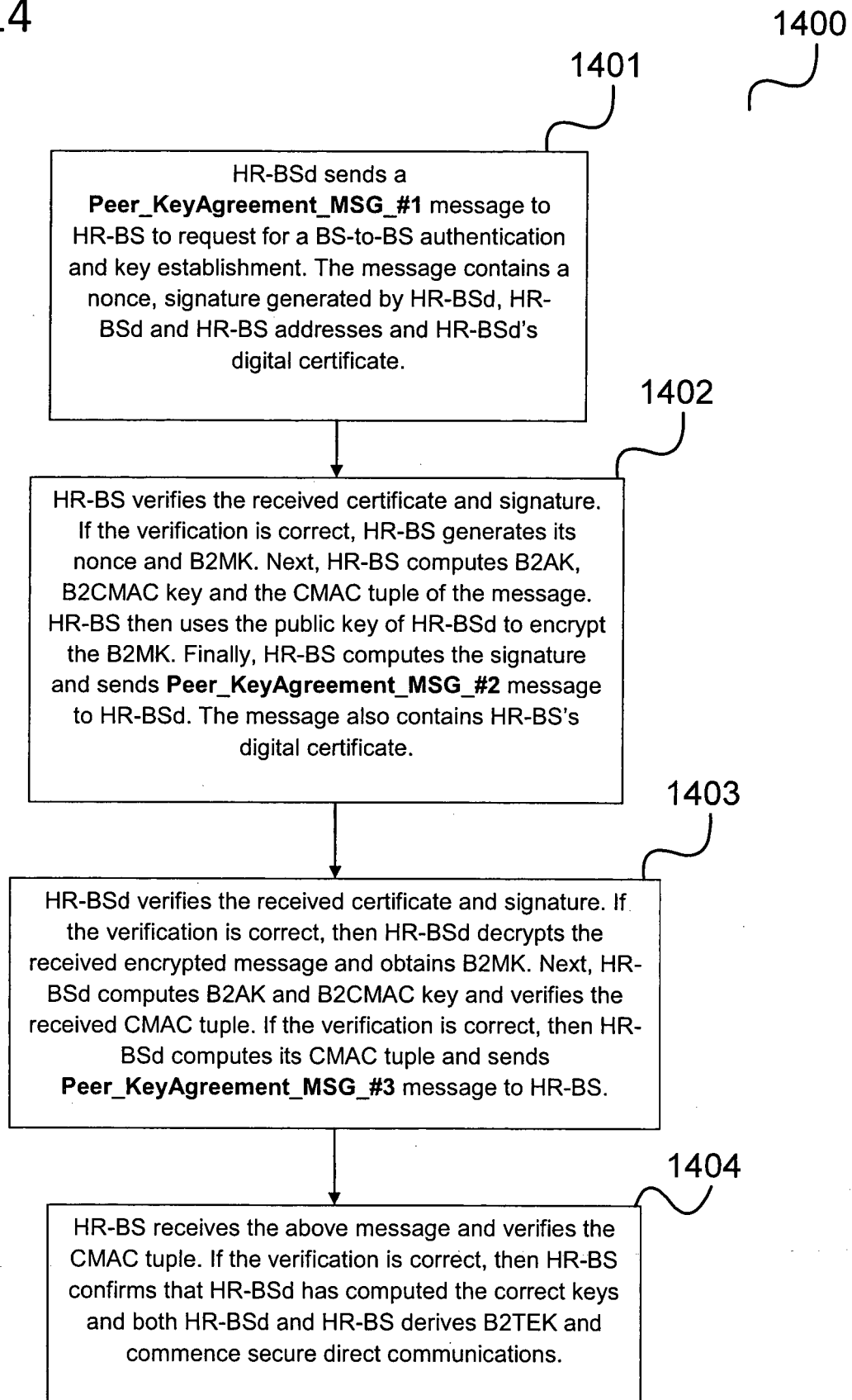


FIG 15

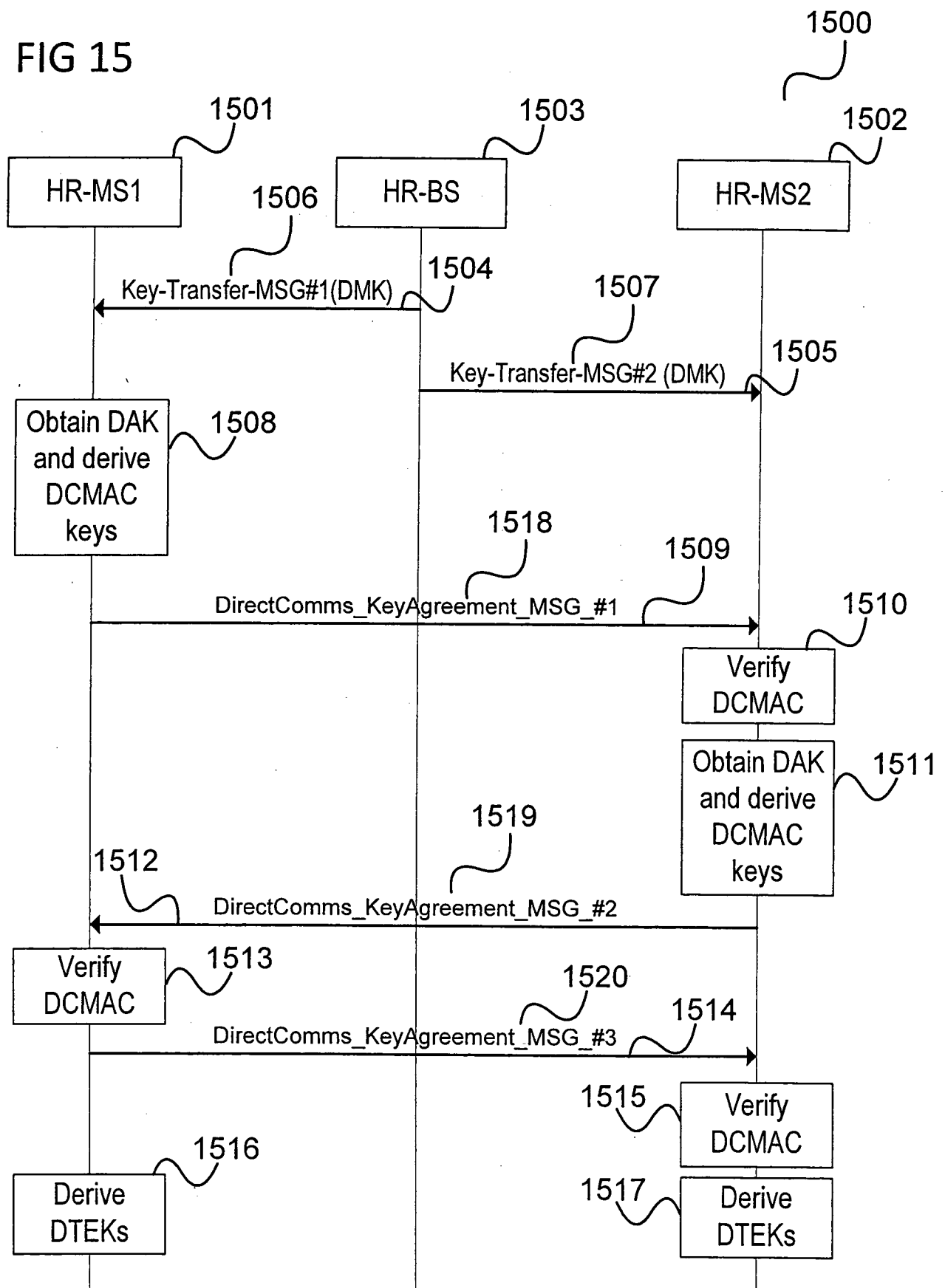
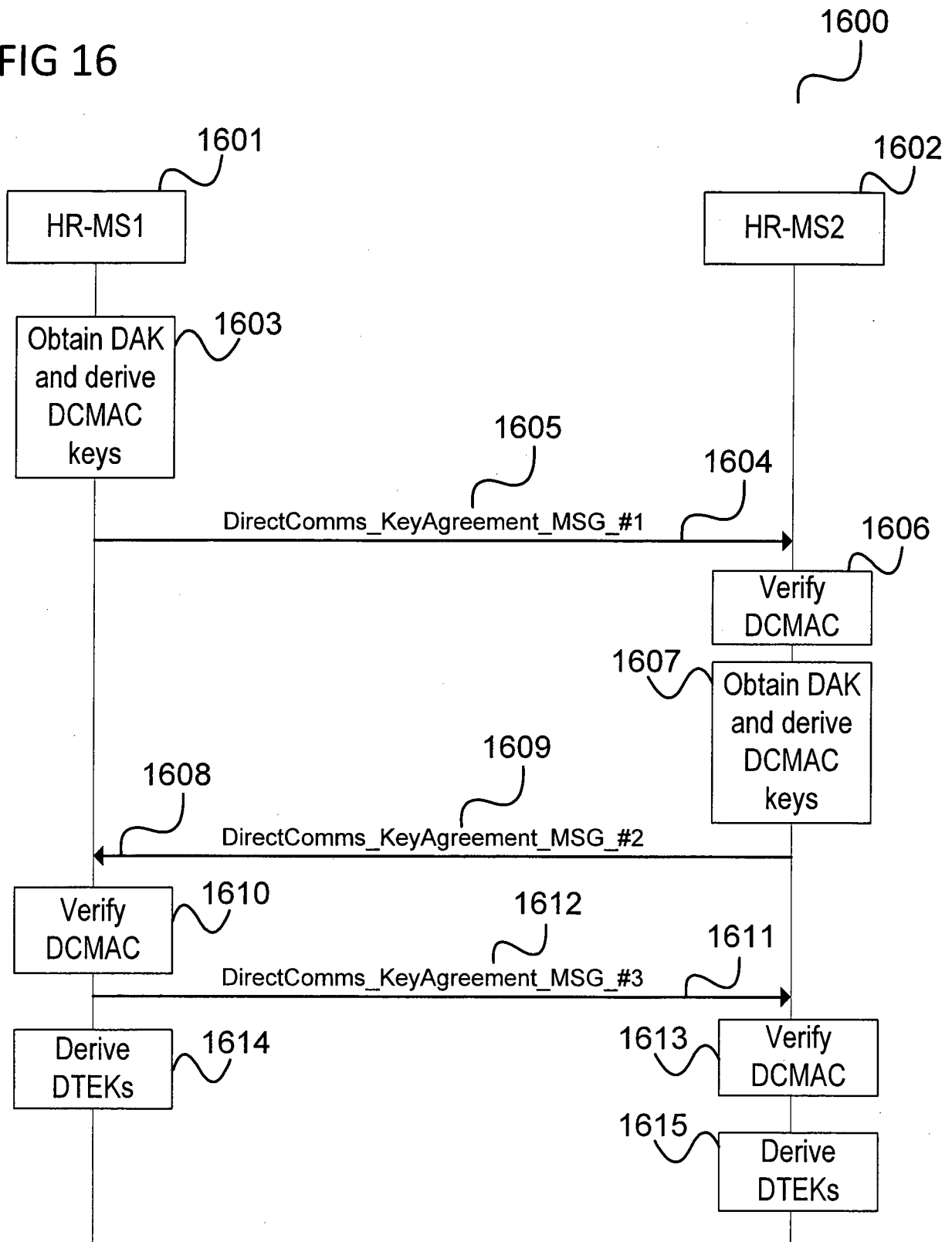


FIG 16



INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2012/000045

A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. H04W 12/04 (2009.01) H04L 9/00 (2006.01) H04W 12/06 (2009.01) According to International Patent Classification (IPC) or to both national classification and IPC				
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPODOC, WPI, Google Scholar, Google Patents: with cellular, mobile, network, communication, secure, encryption, cipher, direct, 802.16, WiMAX, peer to peer, and similar keywords				
C. DOCUMENTS CONSIDERED TO BE RELEVANT				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	US 2006/0087999 A1 (GUSTAVE et al.) 27 April 2006 Abstract; paragraphs [0029]-[0073]; Figs. 2-6	1-22		
X	GUPTA et al., "Decentralized key generation scheme for cellular-based heterogeneous wireless ad hoc networks", Journal of Parallel and Distributed Computing, Vol. 67, No. 9, September 2007, Pages 981-991 Abstract; Sections 3, 4; Figs. 1-4	1-4, 9-11, 20-22		
☐ Further documents are listed in the continuation of Box C ☒ See patent family annex				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed </td> <td style="width: 50%; vertical-align: top;"> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family </td> </tr> </table>			* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family			
Date of the actual completion of the international search 26 March 2012		Date of mailing of the international search report 30 March 2012		
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. +61 2 6283 7999		Authorized officer DR. THAYAPARAN THANABALASINGHAM AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : 61262832238		

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2012/000045

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member			
US	2006087999	CN	1764107	EP	1650915	US	7974234
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.							
END OF ANNEX							