



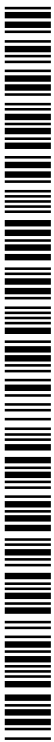
- (51) International Patent Classification:
H04L 9/32 (2006.01)
- (21) International Application Number:
PCT/IB2016/051660
- (22) International Filing Date:
23 March 2016 (23.03.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/139,264 27 March 2015 (27.03.2015) US
- (71) Applicant: CENTRO DE PESQUISAS AVANÇADAS WERNHER VON BRAUN [BR/BR]; Av. Alice de C. Pupo Nogueira Mattosinho, 301, 13098-392 Campinas (BR).
- (72) Inventors: SIEH, Alexander Peter; Rua Marfim, 1317, 13098-354 Campinas (BR). OKADA, Henrique Uemura; Rua Edgar Salviano de Paula, 10, 17511-500 Marília (BR).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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



(54) Title: EMBEDDING PROTECTED MEMORY ACCESS INTO A RFID AUTHENTICATION PROCESS BASED ON A CHALLENGE-RESPONSE MECHANISM

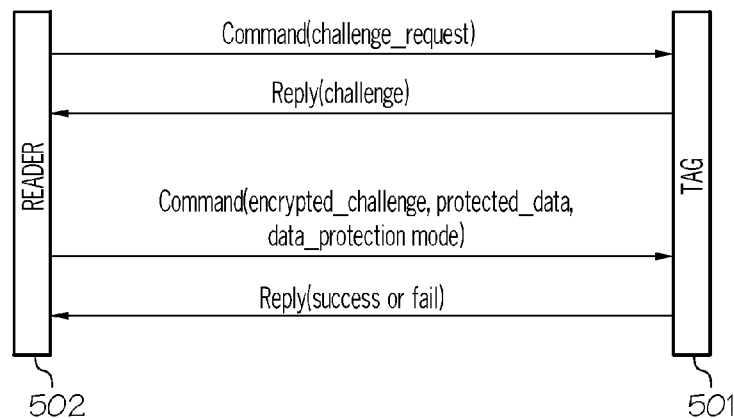


FIG. 16

(57) Abstract: A RFID tag, reader and protocol allow a protected read operation in a two-step tag authentication with cipher-block cryptography. A challenge-response mechanism using a shared secret symmetric key for tag authentication includes a challenge and information to read data from a tag's memory. The tag's response to the challenge-response mechanism includes the response to the reader's challenge and data from the tag's memory. A method embeds a protected write operation in a four-step reader authentication with cipher-block cryptography. The protocol allows a challenge-response mechanism using the shared secret symmetric key for reader authentication including a challenge and information to write data to the tag's memory. The reader's response to the challenge-response mechanism includes a response to the tag's challenge and data for writing to the tag's memory. Authenticated read and write data may be in plaintext, message authentication code (MAC)-protected, encrypted, or both encrypted and MAC protected.

**EMBEDDING PROTECTED MEMORY ACCESS INTO A RFID AUTHENTICATION
PROCESS BASED ON A CHALLENGE-RESPONSE MECHANISM**

5

CROSS REFERENCE TO RELATED APPLICATION

The present application claims priority to U.S. Provisional Application No. 62/139,264 filed on March 27, 2015, which is hereby fully incorporated by reference herein.

10

BACKGROUND

Field

This invention relates generally to a radio frequency identification (RFID) system, and more particularly to a RFID reader, a RFID tag and a RFID protocol.

Related Art

15 An RFID system includes an RFID tag (hereinafter “tag”) and an RFID reader (hereinafter “reader”). The tag comprises an antenna and an integrated circuit. The reader comprises an antenna and circuitry that includes a radio frequency (RF) transmitter and an RF receiver.

RFID technology includes a low frequency band, a high frequency band, an ultra-high frequency (UHF) band, and a microwave band. Each International Telecommunication Union region has
20 its own specific frequency allocation within the UHF band; for example, Europe (Region 1) allocates 866-869MHz, North and South America (Region 2) allocates 902-928MHz, and Asia (Region 3) allocates 950-956MHz. The frequency range 902-928MHz is also referred to as an industrial, scientific and medical (ISM) radio band.

Several standardized methods of cryptography are known. Standardized methods of
25 cryptography include defined ways of processing a data string. Objectives of cryptography include: 1) data confidentiality, i.e., protection against unauthorized disclosure of data; 2) data integrity, i.e., protection that enables the recipient of data to verify that it has not been modified in an unauthorized manner; 3) data origin authentication, i.e., protection that enables the recipient of data to verify the identity of the data originator; 4) non-repudiation, and 5) entity
30 authentication. To achieve these objectives, cryptography may use algorithms for encrypting, hashing, digital signature, etc.

Authenticated encryption is an encryption method which simultaneously provides data confidentiality, data integrity and data origin authentication. An authenticated encryption method, known as encrypt-then-MAC, is defined in ISO/IEC 19772. The term “MAC” is an abbreviation for message authentication code. The encrypt-then-MAC encryption method, which applies a symmetric-key technique, can be incorporated into a conventional RFID transaction wherein a command of a reader instructs a tag to reply, in a ciphertext format, data from its memory with data confidentiality, data integrity and data origin authentication during its tag-to-reader transmission.

FIG. 1 depicts a known example of an authenticated encryption of data to be read from a memory of a tag by a reader. In FIG. 1, after the tag receives a conventional read request (“command”) from the reader, the tag replies. The reply includes the read data from a memory of the tag. The read data is in ciphertext format after applying the authenticated encryption method to the data (for example, encrypt-then-MAC). Then, the reader cryptographically processes the tag’s authenticated encrypted reply to confirm its integrity and data origin and to retrieve the plaintext data.

FIG. 2 depicts a known example of an authenticated encryption of data to be written to the memory of the tag by the reader. In the example shown in FIG. 2, the reader does not send a conventional write request to a tag in plaintext format; instead, the reader applies an authenticated encryption method to the data to be written (for example, encrypt-then-MAC). Then, the reader sends the ciphertext output to the tag. Next, the tag cryptographically processes the reader’s authenticated encrypted message to confirm its integrity and data origin and to retrieve the plaintext data which is to be written into the memory of the tag.

In the examples shown in prior art FIGS. 1 and 2, protected data is provided with confidentiality, integrity and data origin authentication. Reader authentication using the symmetric-key technique is an operation using a cryptographic algorithm over a plurality of parameters. For example, AES-128 in CBC mode can be selected by the data_protection_mode to generate the protected_data.

Entity authentication is an encryption method which verifies that an entity actually is who or what they claim to be. There is a standardized and well-known entity authentication method that is based on a challenge-response mechanism and which is defined in ISO/IEC 9798-2. This challenge-response mechanism requires a claimant and a verifier to share a secret symmetric key (hereinafter “symmetric key”). Then, a claimant and a verifier carry out unilateral entity

authentication using random numbers in two steps. The claimant confirms its identity by demonstrating knowledge of the symmetric key by encrypting a challenge (the random number) using the symmetric key. A conventional communication between a reader and a tag may include a symmetric-key technique.

5 In a RFID system, there are two possible kinds of unilateral entity authentication, one being reader authentication and other being tag authentication. In the current entity authentication methods of UHF RFID protocols, a typical tag authentication procedure begins with a reader sending a challenge to a tag. A challenge from a reader comprises a random number or time-varying data that cannot be anticipated/guessed by an attacker. The challenge from the reader is
10 transmitted to the tag in plaintext. When the reader sends the challenge to the tag for tag authentication purpose, the tag is considered authentic if the tag proves to the reader that the tag has knowledge of the shared symmetric key. Obviously, the tag does so without publicly revealing the symmetric key. To prove to the reader that the tag has knowledge of the symmetric key, the tag encrypts the challenge with the symmetric key and sends the resulting
15 ciphertext. The symmetric key cannot be extracted or inferred from a ciphertext and plaintext pair. Next, the reader decrypts the ciphertext and checks whether the received challenge matches the original challenge sent to the tag. If there is a match, the tag must have used the symmetric key and the tag is authentic.

FIG. 3 depicts a known example of tag authentication using the symmetric-key technique. In the
20 known example shown in FIG. 3, the reader sends its challenge (e.g., a random number) to the tag, and, in response, the tag encrypts the challenge with the symmetric key and replies with ciphertext. This unilateral tag authentication in a UHF RFID protocol takes two steps.

FIG. 4 depicts a known example of reader authentication using the symmetric-key technique. In the known example shown in FIG. 4, as with known UHF RFID protocols, the reader talks first.
25 The reader starts by sending out a challenge request, and, in response, the tag replies with a random number. Then, the reader encrypts the challenge with the symmetric key and transmits its output ciphertext. This unilateral reader authentication in accordance with known RFID protocols takes at least three steps. In the known example shown in FIG. 4, a fourth step is included which the tag confirms to the reader the outcome as being either a successful or an unsuccessful reader
30 authentication.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and is not limited by the accompanying figures, in which like references indicate similar elements. Elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale.

5 FIG. 1 depicts a known example of an authenticated encryption of data to be read from a memory of a tag by a reader.

FIG. 2 depicts a known example of an authenticated encryption of data to be written to a memory of a tag by a reader.

10 FIG. 3 depicts a known example of tag authentication using the challenge-response mechanism with a symmetric-key technique.

FIG. 4 depicts a known example of reader authentication using the challenge-response mechanism with a symmetric-key technique.

FIG. 5 depicts an RFID communication system including a tag and a reader.

15 FIG. 6 is a simplified block diagram of the integrated circuit of a tag in accordance with one embodiment of the invention.

FIG. 7 is a simplified block diagram of the circuitry of a reader in accordance with one embodiment of the invention.

FIG. 8 depicts a simplified internal state diagram of the tag in accordance one embodiment of the invention.

20 FIG. 9 is a functional flow diagram performed at a reader regarding a protected read operation by a reader of data from a tag, in accordance with one embodiment of the invention.

FIG. 10 is a functional flow diagram performed at the tag regarding the protected read operation by the reader of data from the tag, in accordance with one embodiment of the invention.

25 FIG. 11 is a functional flow diagram performed at a reader regarding a protected write operation by the reader of data to a tag, in accordance with one embodiment of the invention.

FIG. 12 is a functional flow diagram performed at the tag regarding the protected write operation by the reader of data to the tag, in accordance with one embodiment of the invention.

FIG. 13 depicts an example, in accordance with one embodiment of the invention, of tag authentication with authenticated encryption of data to be read from a memory of a tag by a reader, and further depicting a command from a reader regarding protected read by the reader of data from the tag, and depicting a reply from a tag to the command.

5 FIG. 14 illustrates an example of the contents of the command shown in FIG. 13.

FIG. 15 illustrates an example of the contents of the reply shown in FIG. 13.

FIG. 16 depicts an example, in accordance with one embodiment of the invention, of reader authentication with authenticated encryption of data to be written to a memory of a tag by a reader, and further depicting a first command from the reader regarding protected write by the reader of data to the tag, a first reply from the tag, a second command from the reader, and a
10 second reply from the tag.

FIG. 17 illustrates an example of the contents of the first command shown in FIG. 16.

FIG. 18 illustrates an example of the contents of the first reply shown in FIG. 16.

FIG. 19 illustrates an example of the contents of the second command shown
15 in FIG. 16.

FIG. 20 illustrates an example of the contents of the second reply shown in FIG. 16.

FIG. 21 illustrates transmissions between a tag and a reader regarding a protected read operation by the reader of data from the tag, in accordance with one embodiment of the invention.

FIG. 22 illustrates transmissions between a reader and a tag regarding a protected write
20 operation by the reader of data to the tag, in accordance with one embodiment of the invention.

DETAILED DESCRIPTION

Known UHF RFID protocols can provide unilateral entity authentication and authenticated encryption of data read or write operation by executing known UHF RFID protocols in
25 sequence, disadvantageously resulting in many steps. The present invention provides unilateral entity authentication and authenticated encryption of data read or write operation in fewer steps, thereby advantageously requiring an exchange of fewer commands and responses between the reader and the tag.

FIG. 5 depicts an RFID communication system **500** which includes at least one RFID tag (hereinafter “tag”) **501** and at least one RFID reader (hereinafter “reader”) **502**. The tag **501** comprises an antenna **513** and an integrated circuit **515**. The reader **502** comprises an antenna **524** and circuitry **526**. The arrow with two arrowheads indicates that the tag **501** and the reader **502** are in two-way wireless communication with each other.

FIG. 6 is a simplified block diagram of the integrated circuit **515** of the tag **501** in accordance with the invention. The integrated circuit **515** includes analog circuitry and combinatorial and sequential digital logic circuitry that form a RF receiver **631**; a RF transmitter **633**; a finite state machine, or state machine logic, **635**; a non-volatile memory (hereinafter “memory”) **637** and a cryptographic engine **639**. The memory **637** stores data and/or a cryptographic key. The combinational and sequential digital logic circuitry controls the RF receiver **631**, the RF transmitter **633**, the memory **637** and the cryptographic engine **639**. In particular, the state machine logic **635** and the cryptographic engine **639** are enhanced compared the state machine logic and the cryptographic engine of known tags. The tag **501** may also include an outer covering, or wrapper, of electrically insulating material.

FIG. 7 is a simplified block diagram of the circuitry **526** of the reader **502** in accordance with the invention. The circuitry **526** includes a RF receiver **740**, and a RF transmitter **742** coupled to a controller **744**. The circuitry **526** also includes an application controller **746** and a cryptographic engine **748** that are coupled to the controller **744**. The application controller **746** may include a microprocessor. The reader **502** is programmed with application software in the application controller **746** and firmware in the controller **744** to accomplish the methods in accordance with the invention.

Every RFID command begins with a command code that identifies a type of RFID command. After the command code, a RFID command may have a message, handle and CRC. In one embodiment, each of the enhanced commands in accordance with the invention replaces a known command code and a known message of a known command with a command code in accordance with the invention and a message in accordance with the invention. In another embodiment, each of the enhanced commands in accordance with the invention replaces only a known message of a known command with a message in accordance with the invention.

FIG. 8 depicts a simplified internal state diagram **800** of a UHF RFID tag, as defined in RFID UHF protocols (for example GS1 EPCGlobal Gen2 protocol or ISO/IEC 18000-63). The tag **501** that implements the methods in accordance with the invention includes the operation of the

internal state diagram **800**. FIG. 8 describes a state flow of a RFID tag according to UHF protocols (GS1 EPCglobal Gen2 or ISO/IEC 18000-63). An RFID tag is controlled by an RFID reader which initiates the communication. The reader (including the reader **502**) instructs the tag (including the tag **501**) to enter several states. A plurality of states including a ready state, an arbitrate state, a reply state, an acknowledged state, an open state, a secured state and a killed state, are illustrated in FIG. 8. Generally speaking, the ready, arbitrate, reply and acknowledged states are preparatory steps for a reader to access a memory of a tag. A reader can only access one tag at a time, and the preparatory steps are necessary in order to singulate one tag from a collection of tags. The tags in the ready state receive a command from the reader and then the tags process the command by practicing an anti-collision arbitration algorithm defined by the UHF protocol specification. The reader's command may cause a tag to either enter the reply state or the arbitrate state. This is a complex singulation procedure performed by tags and readers so as to ultimately allow only one selected tag at a time to transition to other states after the reply state, while other tags wait in the arbitrate state. Once a tag is singulated by the reader, the tag shall be either in the open state or in the secured state. Then, the reader may read or write data from/to the memory of the singulated tag. Moreover, the reader may also send a custom, or enhanced, command. Described herein are enhanced commands and corresponding enhanced replies applied after the singulation phase.

Arbitrate is a possible internal state of the tag **501**. However, as shown in FIG. 8, the internal state of the tag **501** changes according to an exchange of enhanced commands and enhanced replies between the tag **501** and the reader **502**. According to the UHF protocols, the reader **502** always executes the steps for singulation; therefore, during the singulation phase, the tag **501** may transition to the arbitrate state temporarily. Eventually, the tag **501** transitions to the open state or to the secured state. The enhanced commands take place when the tag **501** is in the open state or in the secured state. The steps shown in FIGS. 8 and 10 are executed by the tag **501** only when the internal state of the tag is either in the open state or in the secured state.

FIG. 9 is a functional flow diagram **900** of a method performed at the reader **502** during establishment of a unilateral tag authentication with an embedded protected read operation by the reader **502** of data from the tag **501**. At step **901**, the reader **502** generates a challenge which is part of the enhanced command shown in FIGS. 13 and 14. At step **903**, the reader defines parameters to request a read of data from the memory **637** of the tag **501**. These parameters include the contents of the Data Request fields shown in FIG. 14. At step **905**, the reader **502** defines a configuration parameter for the cryptographic engine **639** of the tag **501** over the

challenge and the defines data to be read from the memory **637**. For example, the reader **502** instructs the tag **501** to execute AES cryptographic engine in CBC mode and in CMAC mode. The configuration parameter is found in the Data Protection Mode field shown in FIG. 14. At step **907**, the reader **502** assembles the enhanced command for transmission. At step **909**, the reader **502** wirelessly transmits the enhanced command to the tag **501**. At step **911**, the reader **502** receives the enhanced reply (see FIGS. 13 and 15) from the tag **501**. The reader **502** performs the unilateral tag authentication with an embedded protected read operation of data from the tag **501** with fewer wireless transmissions between the tag **501** and the reader **502** compared to number of transmissions between a known tag and a known reader when the known reader performs separate unilateral tag authentication and protected read operations.

FIG. 10 is a functional flow diagram **1000** of a method performed at the tag **501** regarding the tag authentication with an embedded protected read operation by the reader **502** of data from the tag **501**. When the tag **501** is singulated by the reader **502**, the tag will be in an open or a secured state. Once a singulation has occurred and the tag **501** is in one of the open or the secured state, the reader **502** and the tag may follow the steps of the method. At step **1002**, the tag **501** receives the enhanced command (see FIG. 13) that was wirelessly transmitted by the reader **502** (see step **909** of FIG. 9). The enhanced command includes a challenge. At step **1004**, the tag **501** examines the parameters of the enhanced command that were defined by the reader **502** at steps **903** and **905**. At step **1006**, based on the Data Request parameters, the tag **501** reads data from its memory **637**. At step **1008**, based on the configuration parameter of the Data Protection Mode, the tag **501** runs its cryptographic engine **639** over the received challenge and over the data from its memory **637**. At step **1010**, the tag **501** assembles the enhanced reply (see FIG. 13) for transmission. At step **1012**, the tag **501** wirelessly transmits the enhanced reply to the reader **502**. The tag **501** performs the unilateral tag authentication with an embedded protected read operation by the reader **502** of data from the tag **501** with fewer wireless transmissions between the tag **501** and the reader **502** compared to number of transmissions between a known tag and a known reader when the known tag performs separate unilateral tag authentication and protected read operations.

Compared with known methods, fewer wireless transmissions are needed between the tag **501** and the reader **502** to accomplish the unilateral tag authentication with an embedded protected read operation by the reader **502** of data from the tag **501**. To accomplish the unilateral tag authentication with an embedded protected read operation, the number of wireless transmissions between the tag **501** and the reader **502** is advantageously only two. The first wireless

transmission is the enhanced command from the reader **502** to the tag **501**, and the second wireless transmission is the enhanced reply from the tag **501** to the reader **502**. On the other hand, the number of transmissions between a known tag and a known reader to accomplish the same task is disadvantageously four. The first wireless transmission is a known command from the known reader to the known tag (for tag authentication). The second wireless transmission is a known reply from the known tag to the known reader (for tag authentication). The third wireless transmission is a known command from the known reader to the known tag (for protected read). The fourth wireless transmission is a known reply from the known tag to the known reader (for protected read).

FIG. 11 is a functional flow diagram **1100** of a method performed at the reader **502** regarding a reader authentication with an embedded protected write operation by the reader **502** of data to the tag **501**. At step **1101**, the reader **502** assembles parameters for a first enhanced command (see FIGS. 16 and 17) for the tag **501**. At step **1103**, the reader wirelessly transmits the first enhanced command to the tag **501**. At step **1105**, the reader **502** wirelessly receives the enhanced reply from the tag **501** (see FIG. 16). The enhanced reply includes a challenge (see FIG. 18). At step **1107**, the reader **502** defines parameters to request a write of data to the tag **501**. At step **1109**, the reader **502** defines a configuration parameter for the cryptographic engine **748** of the reader **502** over the challenge and defines the data that is to be written to the tag **501**. At step **1111**, the reader runs its cryptographic engine **748** to generate a cryptographic block comprising the encrypted tag challenge and the protected data (see FIG. 19) as a result of receiving the challenge from the tag and to generate the protected data that is to be written to the tag **501**. At step **1113**, the reader **502** assembles a second enhanced command (see FIGS. 16 and 19). The second enhanced command includes a configuration parameter and a cryptographic block that contains the challenge and data that is to be written to the tag **501**. At step **1115**, the reader **502** wirelessly transmits the second enhanced command to the tag **501**. At step **1117**, the reader **502** receives a second reply (see FIGS. 16 and 20) from the tag **501**. At step **1119**, the reader **502** examines the second reply the content of which indicates success or failure of the transaction. The reader **502** performs the unilateral reader authentication with an embedded protected write operation of data to the tag **501** with fewer wireless transmissions between the tag **501** and the reader **502** compared to number of transmissions between a known tag and a known reader when the known reader performs separate unilateral reader authentication and protected write operations.

FIG. 12 is a functional flow diagram **1200** of a method performed at the tag **501** regarding the

reader authentication with an embedded protected write operation by the reader **502** of data to the tag **501**. When the tag **501** is singulated by the reader **502**, the tag will be in an open or a secured state. Once singulation has occurred and the tag **501** is in one of the open or the secured state, the reader **502** and the tag may follow the steps of the method. At step **1202**, the tag **501**

5 receives the first enhanced command from the reader **502**. The first enhanced command includes a request for a challenge. At step **1204**, the tag **501** examines the parameters of the first enhanced command. At step **1206**, in response to receiving the first enhanced command, the tag **501** generates an enhanced reply which includes a challenge, and the tag assembles the enhanced reply for transmission. At step **1208**, the tag **501** transmits the enhanced reply to the reader **502**.

10 At step **1210**, the tag **501** receives a second enhanced command from the reader **502**. The second enhanced command includes the configuration parameter and the cryptographic block that contains the data that is to be written to the tag **501**. At step **1212**, the tag **501** examines the configuration parameter. At step **1214**, the tag **501** runs its cryptographic engine **639** over the cryptographic block to obtain, in plain text, the challenge and the data. At step **1216**, the tag **501**

15 determines whether the challenge that was transmitted by the tag is the same as the challenge that was transmitted by the reader **502** and received by the tag. If true, then, at step **1218**, the tag **501** writes the data into its memory **637**, and then, at step **1220**, the tag assembles a success reply for transmission. If false, then, at step **1224**, the tag **501** assembles an error reply for transmission. At step **1222**, the tag **501** transmits one of the success reply and the error reply to

20 the reader **502**. The tag **501** performs the unilateral reader authentication with an embedded protected write operation by the reader **502** of data to the tag **501** with fewer wireless transmissions between the tag **501** and the reader **502** compared to number of transmissions between a known tag and a known reader when the known tag performs separate unilateral reader authentication and protected write operations.

25 Compared with known methods, fewer wireless transmissions are needed between the tag **501** and the reader **502** to accomplish the unilateral reader authentication with an embedded protected write operation by the reader **502** of data to the tag **501**. To accomplish the unilateral reader authentication with an embedded protected write operation, the number of wireless transmissions between the tag **501** and the reader **502** is advantageously only four. The first

30 wireless transmission is the first enhanced command from the reader **502** to the tag **501**. The second wireless transmission is the first enhanced reply from the tag **501** to the reader **502**. The third wireless transmission is the second enhanced command from the reader **502** to the tag **501**. The fourth wireless transmission is the second enhanced reply from the tag **501** to the reader **502**. On the other hand, the number of transmissions between a known tag and a known reader

to accomplish the same task is disadvantageously six. The first wireless transmission is the first command from the known reader to the known tag (for reader authentication). The second wireless transmission is the first reply from the known tag to the known reader (for reader authentication). The third wireless transmission is the second command from the known reader to the known tag (for reader authentication). The fourth wireless transmission is the second reply from the known tag to the known reader (for reader authentication). The fifth wireless transmission is the third command from the known reader to the known tag (for protected write). The sixth wireless transmission is the third reply from the known tag to the known reader (for protected write).

10 The methods in accordance with the invention combine two of the prior art examples described earlier. One prior art example is a method of authenticated encryption to add cryptographic security (hereinafter “security”) to data, which is shown in FIG. 1 or FIG. 2. The other prior art example is a unilateral authentication based on challenge-response mechanism and symmetric-key techniques shown in FIG. 3 or in FIG. 4. The prior art example of the method of

15 authenticated encryption to add security to data shown in FIG. 1 can be combined with the prior art unilateral authentication based on challenge-response mechanism and symmetric-key techniques shown in FIG. 3. The prior art example of the method of authenticated encryption to add security to data shown in FIG. 2 can be combined with the prior art example of unilateral authentication based on challenge-response mechanism and symmetric-key techniques shown in

20 FIG. 4.

The request of information from or to the memory of the tag **501** is an independent and distinct parameter of a command from the reader **502**, and the tag does not send back the request for information to the reader.

The challenge should have characteristics that minimize occurrences in which a reader re-sends the same stream of bits to a tag for authentication purposes to make it less likely that an attacker who does not have knowledge of the symmetric key could reuse a previous observed and successful authentication transaction. If an attacker did observe and record a previous successful authentication transactions, then, when a reader reuses the same value for a challenge, the attacker could transmit the recorded ciphertext and be authenticated, which is a security breach.

25

30 Therefore, to avoid a quick and low-cost “replay attack” from occurring, a challenge is usually a random number or time-varying data with large enough range such that the challenge cannot be guessed or be exhaustively recorded by an attacker. Consequently, the challenge may consist of

solely the random number or time-varying data. In another embodiment, the challenge may consist of the random number or time-varying data plus a request for information to read/write data to/from the memory of a tag.

Embedding a protected read operation in a two-step tag authentication
with cipher-block cryptography

5

The RFID communication system **500** may use an enhanced read command in accordance with the invention. The enhanced read command includes not only a challenge but also information, in plaintext, requesting a read operation from the memory **637** of the tag **501**.

10 In the RFID communication system **500**, tag authentication can be achieved by means of a two-step challenge-response mechanism using symmetric-key cryptography. See FIG. 13.

A first step of tag authentication comprises the reader **502** transmitting the enhanced read command. Unlike the known read command shown in FIG. 1, the enhanced read command includes a tag authentication challenge (hereinafter “challenge”), to the tag **501**. See FIG. 14. A challenge comprises, in plaintext, a random number or time-varying data, generated by the
15 reader **502**. The enhanced read command includes all information needed for requesting the data that is to be read from the memory **637** of the tag **501**. The enhanced read command includes information requesting a data protection mode for transmission of an enhanced reply from the tag **501**. The data protection mode comprises a key pointer, a key size, a cryptographic algorithm selector and a cryptographic protection mode selector. In one embodiment, the data
20 protection mode is the same symmetric-key and block-cipher mode used for the challenge-response component of tag authentication portion of the enhanced read command. In other embodiments, the data protection mode may be implied and not be explicitly configured in the enhanced read command signal. In still other embodiments, the data protection mode used for the data read from the memory of the tag may be a different data protection mode than the data
25 protection mode used for the challenge-response component of tag authentication.

A second step of tag authentication comprises the tag **501** transmitting an enhanced reply to the challenge. See FIG. 15. Unlike the known reply to the known read command shown in FIG. 1, a correct enhanced reply to the enhanced command comprises a correct encryption by the tag
30 **501** of the received challenge with a specific symmetric key that has been shared between the tag and the reader **502** that are in communication with each other. A correct transmission by the tag **501** of the enhanced reply to the challenge from the reader **502** results in a successful

authentication of the tag. With the method, the enhanced reply of the tag **501** comprises at least two components, one being the encrypted response to the challenge, and the other component being the data read from the memory **637** of the tag in the data protection mode that was requested by the reader **502**. Authenticated read information requested by the reader **502**,
5 implicitly or not, may be in plaintext, MAC protected, encrypted, or encrypted and MAC protected.

**Embedding a protected write operation in a four-step reader authentication
with cipher-block cryptography**

In the RFID communication system **500**, reader authentication can be achieved by means of a
10 four-step challenge-response mechanism using symmetric-key cryptography. FIG. 16 shows a series of transmissions between the reader **502** and the tag **501**, initiated by the reader, in which the reader authenticates its identity to the tag and also writes data to the memory **637** of the tag via an encrypted wireless transmission.

A first step of authentication comprises an enhanced command from the reader **502** which
15 requests a challenge from the tag **501**. See FIG. 17. A second step comprises the enhanced reply from the tag **501**. The enhanced reply includes a challenge to the reader **502** in plaintext. See FIG. 18. The challenge from the tag **501** comprises in plaintext, a random number or time-varying data, generated by the tag.

A third step of reader authentication comprises the reader **502** transmitting the enhanced write
20 command to the tag **501**. Unlike the known write command shown in FIG. 2, the enhanced write command shown in FIG. 19 includes not only the write request for writing data into the memory **637** of the tag **501**, but also a correct encryption by the reader **502** of the received challenge with a specific symmetric key that has been shared between the reader and the tag that are in communication with each other. The enhanced write command includes all information
25 needed for writing data to the memory **637** of the tag **501**. The enhanced write command includes, in plaintext, all necessary information identifying the data protection mode that was used by the reader **502** to encrypt the data which is to be written in the memory **637** of the tag **501**. In one embodiment, the data protection mode is based on the same symmetric-key and block-cipher mode used for the challenge-response component of the reader authentication. In
30 another embodiment, the data protection mode may be implied and not be explicitly configured by the enhanced command from the reader **502**. In still another embodiment, the data protection mode of the data written to the memory **637** of the tag **501** may also use a different symmetric-

key or block-cipher mode than the challenge-response component of the reader authentication.

A fourth step of authentication is a reply from the tag **501** that indicates either a success or a failure of the reader's authentication and/or protected write operation. See FIG. 20.

5 With the method in accordance with the invention, the sequence, position, quantity and length of the parameters that comprise the enhanced command from the reader **502** or the enhanced reply from a tag **501** are not fixed.

In one embodiment, an enhanced command from the reader **502** has a configuration parameter defining the data protection mode of the data operation. If not explicit, the configuration parameter is implied by the protocol. If explicit, the reader **502** is capable of choosing any one
10 of the data protection modes in any given enhanced challenge-response authentication procedure.

In one embodiment, an enhanced command from the reader **502** has configuration parameters defining the key pointer, the key size, the cryptographic algorithm or the cryptographic protection mode to be used in the protection of the data operation. If not explicit, the
15 configuration parameters are implied by the protocol and cannot be altered. If explicit, the reader **502** is capable of choosing a specific symmetric key, cryptographic algorithm and data protection mode in any given enhanced challenge-response authentication procedure.

In one embodiment, an enhanced command from the reader **502** instructs a data protection mode on the tag data that involves confidentiality based on a cryptographic mode of operation. In
20 another embodiment, an enhanced command from the reader **502** instructs the data protection mode on the data that involves generating a MAC for integrity purposes based on a cryptographic mode of operation. In still another embodiment, a reader's command instructs the data protection mode on the data that involves both confidentiality and generation of a MAC for integrity purposes based on a single or multiple cryptographic modes of operation. In yet
25 another embodiment, an enhanced from the reader **502** instructs the data protection mode on the tag data that does not involve any special cryptographic operation, allowing the transmission of the data in plaintext format.

In one embodiment, an enhanced command from the reader **502** has another configuration parameter defining whether its datagram includes a data operation at all. If the data operation is
30 not required, the procedure collapses down to a generic tag/reader authentication procedure which means that a reply from the tag **501** or a command from a reader **502** does not include any

protected data at all.

In one embodiment, an enhanced command from the reader **502** instructs protected data to be written to the memory of the tag **501** in which such protected data constitutes part of, or an entire, cryptographic key.

5 An example of an embodiment of the method in accordance with the invention is shown in FIGS. 13, 14 and 15.

FIG. 13 depicts an example, in accordance with one embodiment of the invention, of authenticated encryption of data to be read from the memory of the tag **501** by the reader **502**, and further depicting the enhanced command from the reader regarding protected read by the reader of data from the tag, and depicting the enhanced reply from the tag to the enhanced
10 command.

FIG. 14 depicts the enhanced command from the reader **502** and its message contents during a tag authentication with embedded protected read. A Data Request consists of a Data Include Enable field, a Pointer field and a Word Count field. The reader challenge field contains only a
15 random number or time-varying data. The enhanced command also includes a command code, a message, a handle and a CRC. The command code specifies a command type and the message contains the information necessary to execute the command. The handle is a number that allows the reader **502** to specify a particular tag **501** from among a plurality of tags, each of which may have a different handle, and the CRC is an error-check code that allows the tag to check the
20 command for errors. Each of these fields is described in more detail in the GS1 EPCglobal Gen2 specification or in the ISO/IEC 18000-63 standard.

FIG. 15 depicts the enhanced reply from the tag **501** and contents (“RESP”) of the enhanced reply during a tag authentication with embedded protected read. The RESP portion of the enhanced reply from the tag **501** includes data that confirms the authenticity of the tag **501**. The
25 tag **501** confirms its authenticity by including, in the RESP portion of the enhanced reply, the reader's challenge in ciphertext format. The RESP portion of the enhanced reply from the tag **501** also includes encrypted data from the memory of the tag. The encrypted reader challenge field contains the content of the reader challenge field after the content has been encrypted with the shared symmetric key.

30 FIG. 16 depicts an example, in accordance with one embodiment of the invention, of an authenticated encryption of data to be written to the memory of the tag **501** by the reader **502**,

and further depicting an enhanced command from the reader regarding protected write by the reader of data from the tag, a challenge from the tag, a response to the challenge, and the enhanced reply from the tag.

FIG. 17 illustrates an example of the contents of the enhanced command shown in FIG. 16 during a reader authentication procedure with embedded protected write. The enhanced
5 command includes a message portion. The enhanced command is used during a step when the reader **502** requests a challenge from the tag **501**. The Request Tag Challenge field contains control information that requests the tag **501** to generate and send its challenge to the reader **502**. The control information may be considered unnecessary in an embodiment in which a dedicated
10 code for the enhanced command is used in this step. In such case, the message portion of the enhanced command could be empty.

FIG. 18 illustrates an example of the contents of the challenge from the tag **501** shown in FIG. 16. FIG. 18 illustrates the enhanced reply from the tag **501** including a first RESP from the tag during a reader authentication with embedded protected write. The Tag Challenge field contains
15 only a random number or time-varying data.

FIG. 19 illustrates an example of the contents of the response to the challenge shown in FIG. 16. FIG. 19 illustrates an example of the enhanced command from the reader **502** and its second message contents during a reader authentication procedure with embedded protected write. In one embodiment, the parameter Data Request could be avoided if such functionality is always
20 implicit and imposed by the enhanced command, so in such embodiment of the disclosure, this parameter is avoided in the message field. Similarly, the parameter Data Protection Mode could also be avoided if such functionality is always implicit and imposed in a specific embodiment. In another embodiment, a proposed command could define that the parameter Pointer and the parameter Word Count should also be encrypted according to Data Protection Mode as well,
25 instead of being transmitted in plaintext format. Moreover, the order of any parameters inside the message portion of the enhanced command could be changed. It is foreseeable that any parameters could be broken into subparts (split) and rearranged.

As mentioned previously, the parameter "Data Protection Mode" may include control/configuration information for the protection of the data, including, but not limited to:
30 definition of which cryptographic algorithm to be used, key pointer, key size, and the selection of the cryptographic protection mode used such as confidentiality only (CBC), integrity only (CMAC), confidentiality with integrity (CBC+CMAC) or simply plaintext (no cryptography).

FIG. 20 illustrates an example of the contents of the enhanced reply from the tag **501** shown in FIG. 16 including a second RESP from the tag during a reader authentication procedure with embedded protected write. If the write operation or authentication step fails, the tag **501** replies with an error header and the RESP may include an error code to identify the specific type of error. Otherwise, if succeeded, the tag **501** replies with a success header and the RESP may be empty as there is no need to send any further information to the reader **502**.

Embodiments of the method for tag authentication with protected read operation

FIG. 21 depicts four (4) embodiments of the method for tag authentication with protected read in accordance with the invention. FIG. 21 also depicts, for comparison purposes, the content of a known response from a known tag.

“RESP_PRIOR” is a known challenge-response tag authentication: no RDATA is read from a memory of the known tag.

“RESP_A” is tag authentication and reading RDATA from the memory **637** of the tag **501** in accordance with one embodiment of the method, wherein RDATA is plaintext data.

“RESP_B” is tag authentication and reading RDATA from the memory **637** of the tag **501** in accordance with another embodiment of the method, wherein RDATA is plaintext data followed by a MAC calculated using AES-128 CMAC mode.

“RESP_C” is tag authentication and reading RDATA from the memory **637** of the tag **501** in accordance with yet another embodiment of the method, wherein RDATA is cryptographed data in AES-128 CBC encryption mode.

“RESP_D” is tag authentication and reading RDATA from the memory **637** of the tag **501** in accordance with still another embodiment of the method, wherein RDATA is cryptographed data in AES-128 CBC encryption mode followed by a MAC calculated using AES-128 CMAC mode.

The order of parameters within message or RESP portions of the command may be changed. Inasmuch as CFG may be implied and fixed by a protocol version, CFG, CONST and RAND are optional parameters.

Embodiments of the method for reader authentication with protected write operation

FIG. 22 depicts four (4) embodiments of the method for reader authentication with protected write in accordance with the invention. FIG. 22 also depicts, for comparison purposes, the content of a known response from a known reader.

5 “MESSAGE2_PRIOR” is a known challenge-response interrogator authentication: no WDATA is written to a memory of a known tag.

“MESSAGE2_A” is a reader authentication with writing WDATA to the memory **637** of the tag **501** in accordance with one embodiment of the invention, wherein WDATA is plaintext data.

10 “MESSAGE2_B” is a reader authentication with writing WDATA to the memory **637** of the tag **501** in accordance with another embodiment of the invention, wherein WDATA is plaintext data followed by a MAC calculated using AES-128 CMAC mode.

“MESSAGE2_C” is a reader authentication with writing WDATA to the memory **637** of the tag **501** in accordance with yet another embodiment of the invention, wherein WDATA is cryptographed data in AES-128 CBC decryption mode.

15 “MESSAGE2_D” is a reader authentication with writing WDATA to the memory **637** of the tag **501** in accordance with still another embodiment of the invention, wherein WDATA is cryptographed data in AES-128 CBC decryption mode followed by a MAC calculated using AES-128 CMAC mode.

20 The order of parameters within message or RESP portions of the enhanced command may be changed. Because CFG may be implied and fixed by a protocol version, CFG, CONST and RAND are optional parameters.

The methods in accordance with the invention advantageously achieve authentication and a combination of: 1) data confidentiality, 2) data integrity, and 3) data origin authentication.

25

Definition of terms and abbreviations

Encryption: the conversion of data into a form called a ciphertext that cannot be easily understood by unauthorized people.

Cipher-block cryptography: cryptography based on block cipher, as opposed to cryptography based on stream ciphers.

Symmetric-key technique: a technique that uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext, as opposed to asymmetric-key techniques where the cryptographic key for encryption is different from the one for decryption.

5 Cryptographic key: a string of bits used by a cryptographic algorithm to transform plaintext into ciphertext or vice versa. This key remains private and ensures secure communication.

Message: a parameter or a plurality of parameters inside a command from a reader.

RESP: a parameter or a plurality of parameters inside a reply from a tag.

CFG: a collection of configuration parameters that:

selects if additional data in response is present, e.g., the data request of FIG. 13;

10 selects if the additional data is cryptographically protected with confidentiality, e.g., the data protection mode of FIG. 13;

selects if the additional data is cryptographically protected by a MAC, e.g., the data protection mode of FIG. 13;

15 selects if the additional data is cryptographically protected by a MAC and with confidentiality, e.g., the data protection mode of FIG. 13;

selects if the additional data is in plaintext format, e.g., data protection mode of FIG. 13;

selects the memory position and length of the additional data, e.g., the pointer and word count of FIG. 13;

20 selects a key for use in the cryptographic operation, e.g., the data protection mode of FIG. 13; and

selects if the WDATA is a data value or a key update value, e.g., the pointer, the word count and the data protection mode of FIG. 19.

CBC: cipher block chaining, a block cipher mode defined in NIST SP800-38A.

CMAC: block cipher-based message authentication code (as described in NIST SP800-38B).

25 CONST: constant number (optional).

PC: protocol control word that mainly defines the number of words of UII/EPC (see GS1 EPCGlobal Gen2 protocol or ISO/IEC 18000-63).

RAND: random number (optional).

RDATA: additional data read from memory.

30 RN16: 16-bit random or pseudo-random number (see GS1 EPCGlobal Gen2 protocol or ISO/IEC 18000-63).

WDATA: additional data to write to memory or new key value.

AES: advanced encryption standard, a block cipher defined in FIPS PUB 197 and ISO/IEC 18033-3.

- 5 AES-128: AES block cipher using a 128-bit key.

ICH: interrogator challenge (also known as reader challenge).

TCH: tag challenge.

UII/EPC: code that identifies the object to which a tag is affixed (see GS1 EPCGlobal Gen2 protocol or ISO/IEC 18000-63).

10

What is claimed is:

CLAIMS

1. A method at a RFID tag, comprising:
5 wirelessly receiving a challenge from a RFID reader; and
wirelessly transmitting, in a single transmission, an authentication of the challenge and
data from a memory of the RFID tag.
- 10 2. The method at a RFID tag of claim 1, wherein the single transmission is performed in
response to the challenge.
3. The method at a RFID tag of claim 2, wherein the challenge includes a request for
15 information from the memory of the RFID tag.
4. A method at a RFID reader, comprising:
wirelessly receiving a challenge from a RFID tag; and
20 wirelessly transmitting, in a single transmission, an authentication of the challenge and
data to be written to a memory of the RFID tag.
5. The method at a RFID reader of claim 4 wherein the single transmission is performed in
25 response to the challenge.
6. The method at a RFID reader of claim 4, wherein, prior to the step of wirelessly
receiving a challenge from a RFID tag, the step of the RFID reader wirelessly transmitting a
30 request for the challenge from the RFID tag.

7. A method for performing a protected read operation in a RFID system, comprising:
a reader transmitting an enhanced read command to a tag, the enhanced read command including a challenge and a request for data from a memory of the tag, the request for data
5 including all information needed for identifying the data that is to be read from the memory of the tag, the information also including a cryptographic data protection mode for transmission of an enhanced reply from the tag;
the tag transmitting the enhanced reply to the challenge, the enhanced reply comprising at least two components:
10 a correct encryption and transmission of the challenge, in ciphertext, using a specific symmetric-key that was previously shared between the tag and the reader, and
encrypted data from the memory of the tag, the data having been encrypted using the data protection mode that was requested by the reader.
- 15
8. A method for performing a protected write operation in a RFID system, comprising:
a reader transmitting a command signal that includes a request for a challenge from a tag;
the tag transmitting an enhanced reply to the request for a challenge, the enhanced reply including the challenge in plaintext, the challenge including a random number generated by the
20 tag;
the reader transmitting an enhanced write command to the tag, the enhanced write command including:
a response to the challenge,
encrypted data that is to be written to a memory of the tag, and
25 information, in plaintext, needed for writing the encrypted data to the memory of the tag, the information including identifying a data protection mode that was used to encrypt the data.
9. The method of claim 8, including the step of:
30 the tag transmitting a second response, the second response including information indicating whether the protected write operation succeeded or failed.

10. A RFID tag, comprising:
a radio frequency receiver and transmitter;
circuitry, coupled to the radio frequency receiver and transmitter;
5 a memory, coupled to the circuitry, for storing data and a cryptographic key; and
a cryptographic engine, coupled to the circuitry, for performing cryptographic
operations,
wherein the RFID tag transmits, in a single transmission, an authentication of a challenge
from a RFID reader to the RFID tag and data from a memory of the RFID tag.
- 10
11. The RFID tag of claim 10, wherein the circuitry includes combinational and sequential
digital logic circuitry.
- 15
12. The RFID tag of claim 11, wherein the combinational and sequential digital logic
circuitry includes state machine logic.
- 20 13. A RFID reader, comprising:
a radio frequency receiver and transmitter; and
circuitry, coupled to the radio frequency receiver and transmitter, wherein the RFID
reader wirelessly transmits, in a single transmission, an enhanced write command to a RFID tag,
the enhanced write command including:
25 a response to a challenge from the RFID tag,
encrypted data that is to be written to a memory of the RFID tag, and
information, in plaintext, needed for writing the encrypted data to the memory of the
RFID tag, the information including identifying a data protection mode that was used to encrypt
the data.

14. The RFID reader of claim 13, wherein the circuitry includes combinational and sequential digital logic circuitry.

5 15. The RFID reader of claim 14, wherein the combinational and sequential digital logic circuitry includes state machine logic.

16. The RFID reader of claim 13, wherein the circuitry includes a processor and a memory for storing instructions for execution by the processor.

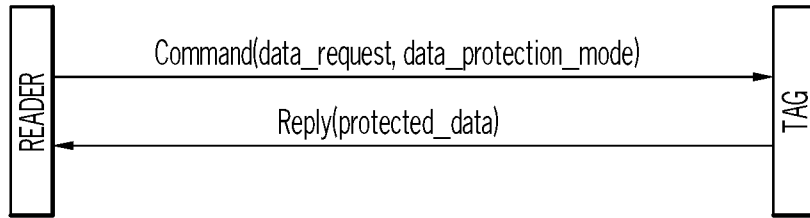


FIG. 1 (PRIOR ART)

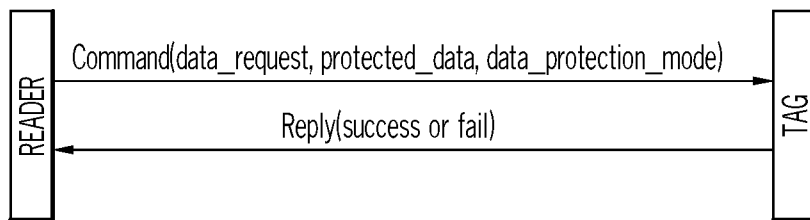


FIG. 2 (PRIOR ART)

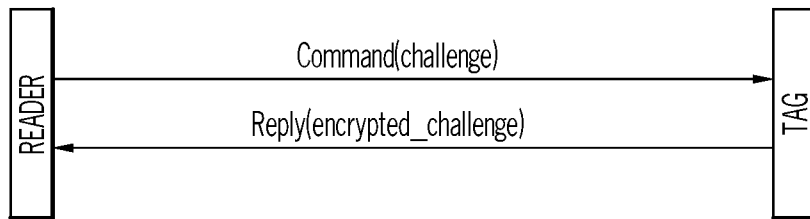


FIG. 3 (PRIOR ART)

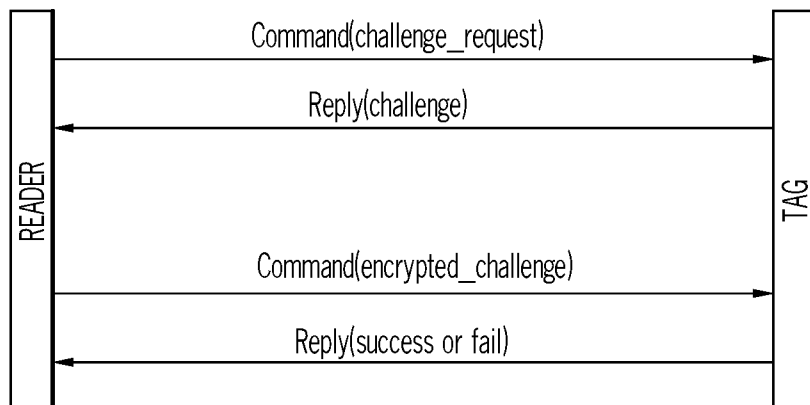


FIG. 4 (PRIOR ART)

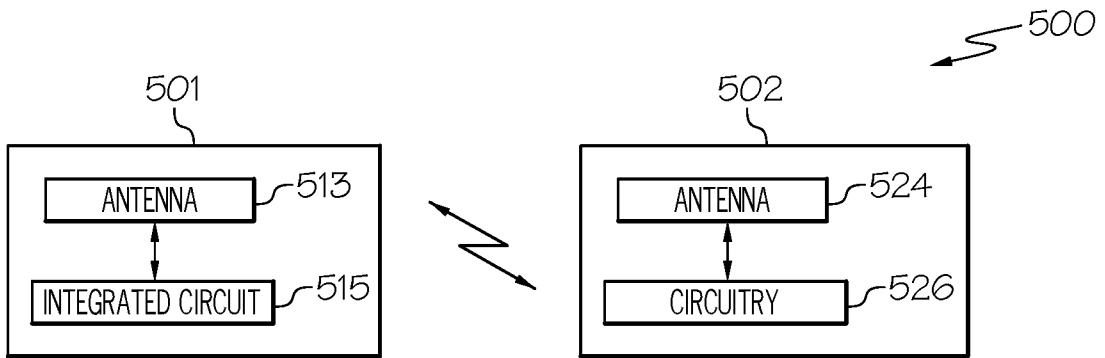


FIG. 5

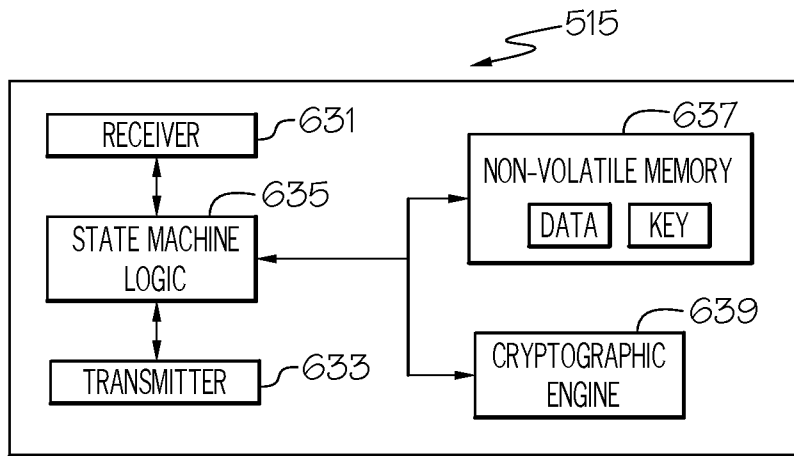


FIG. 6

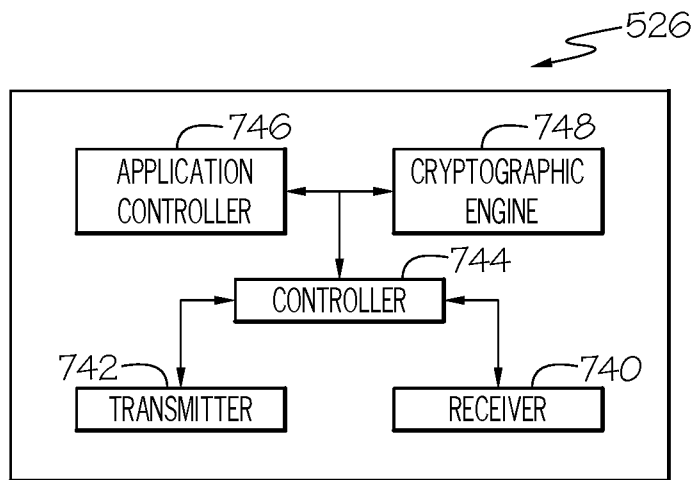


FIG. 7

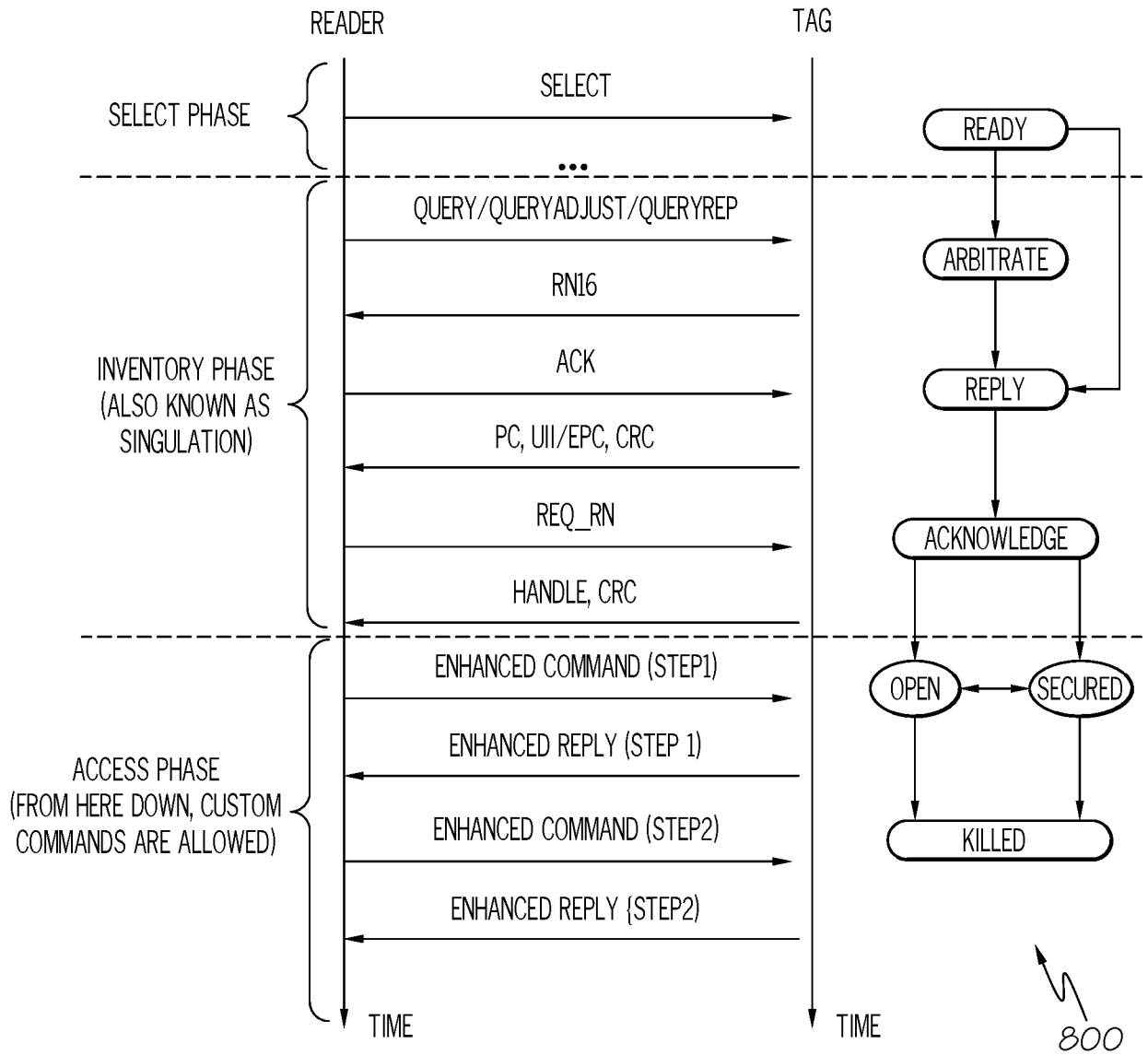


FIG. 8

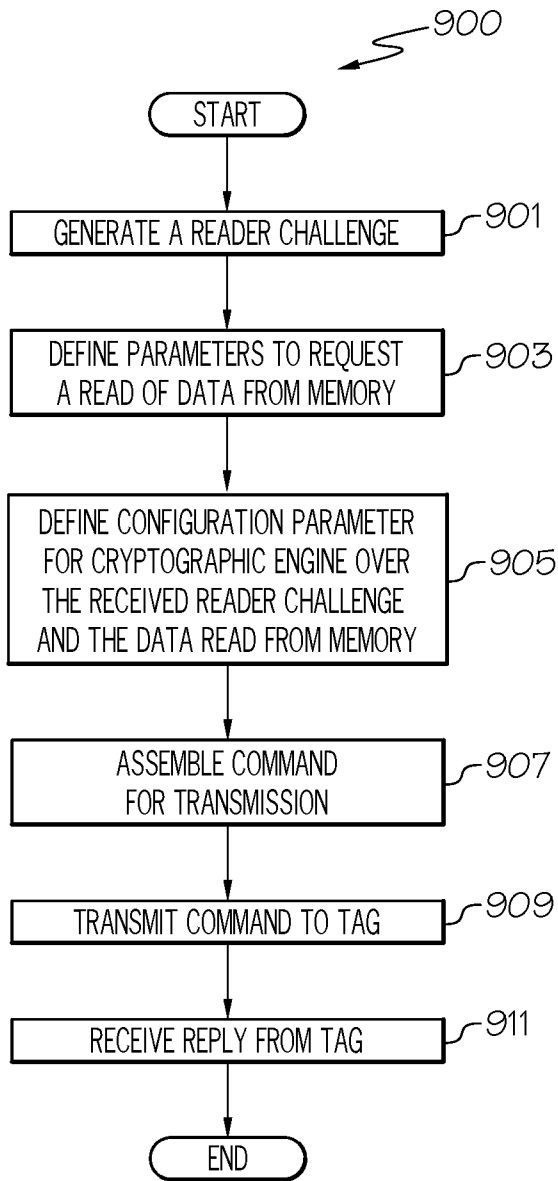


FIG. 9

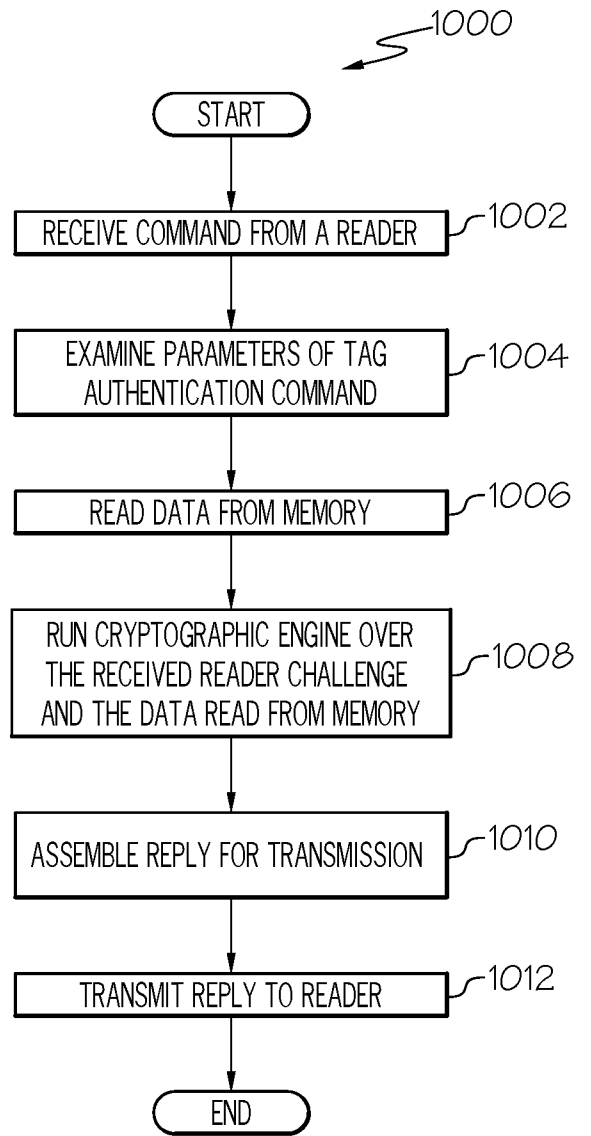


FIG. 10

5 / 10

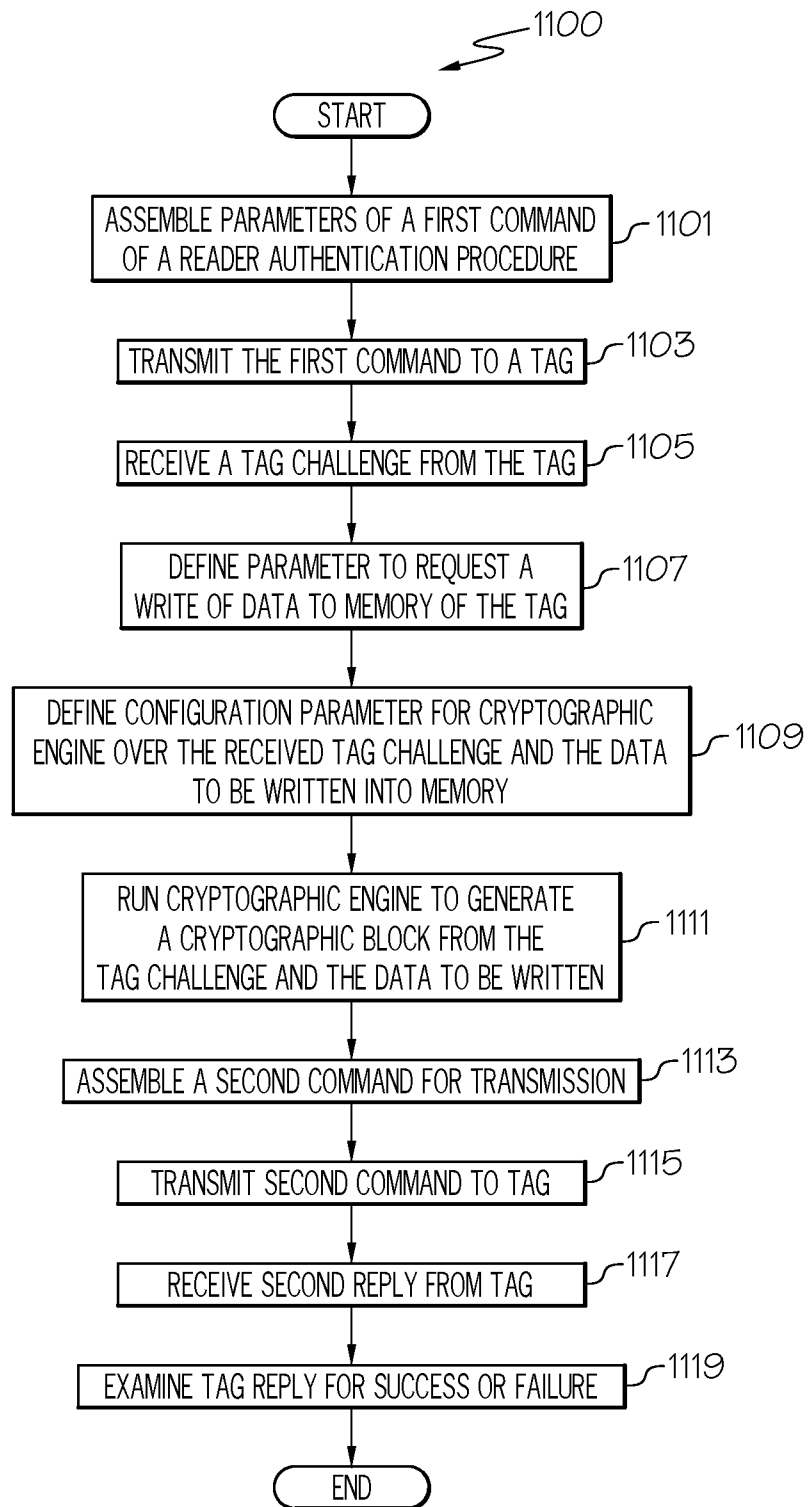


FIG. 11

6 / 10

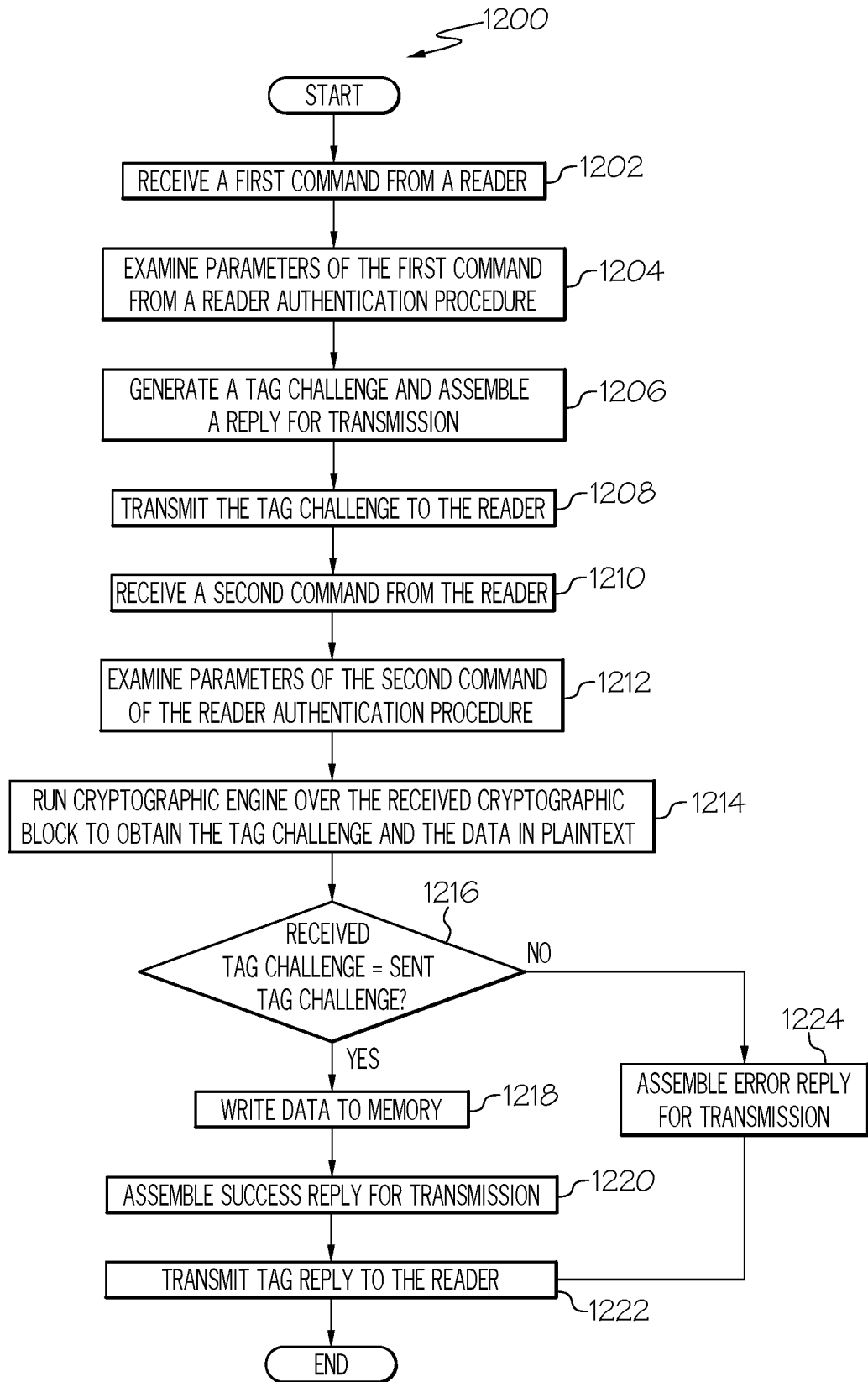


FIG. 12

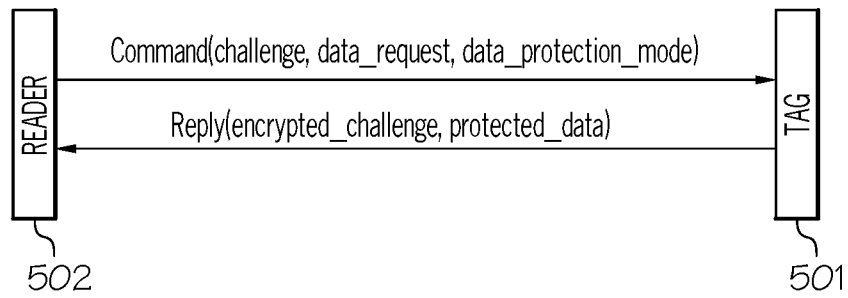


FIG. 13

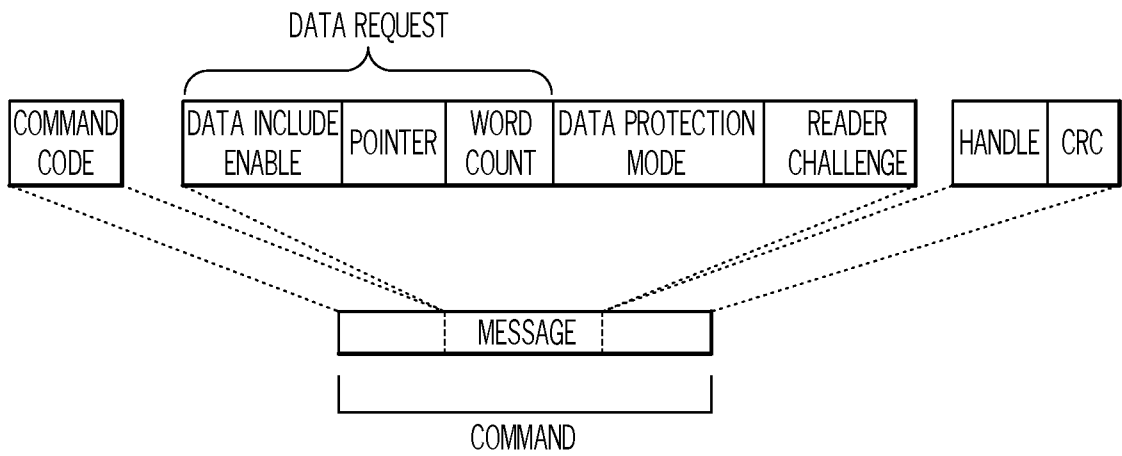


FIG. 14

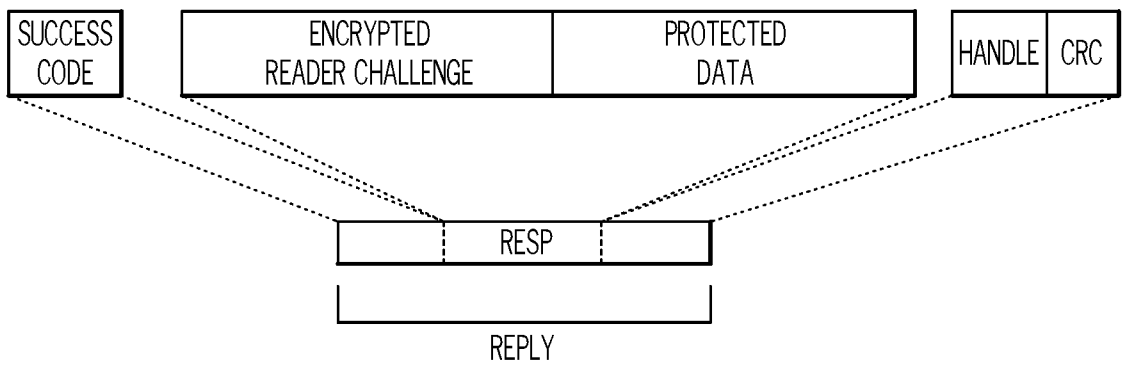


FIG. 15

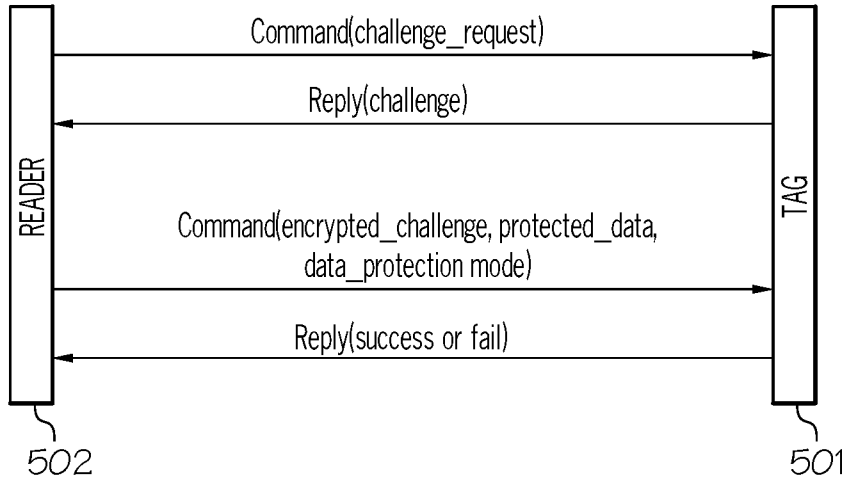


FIG. 16

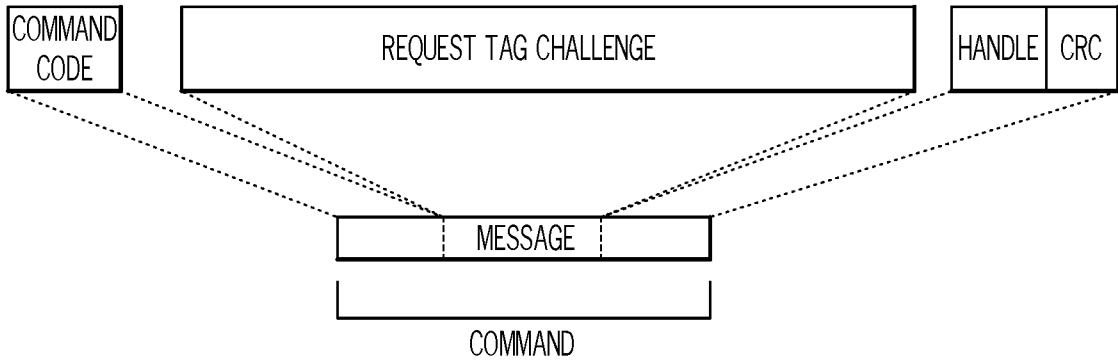


FIG. 17

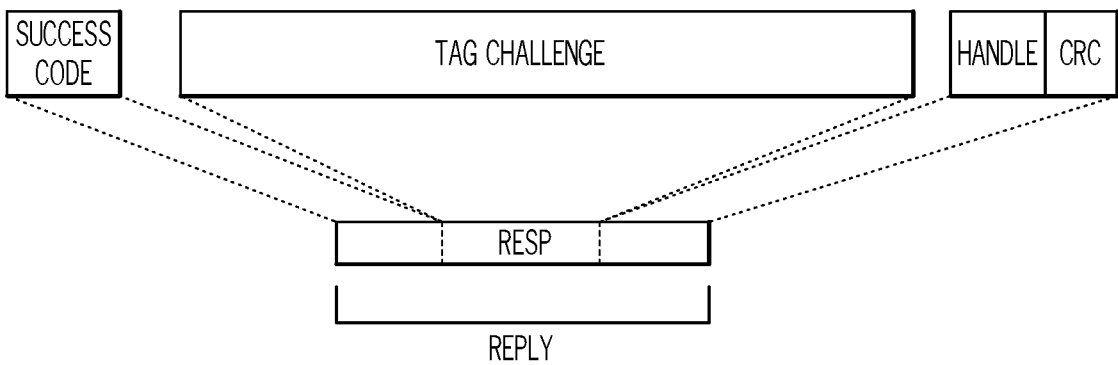


FIG. 18

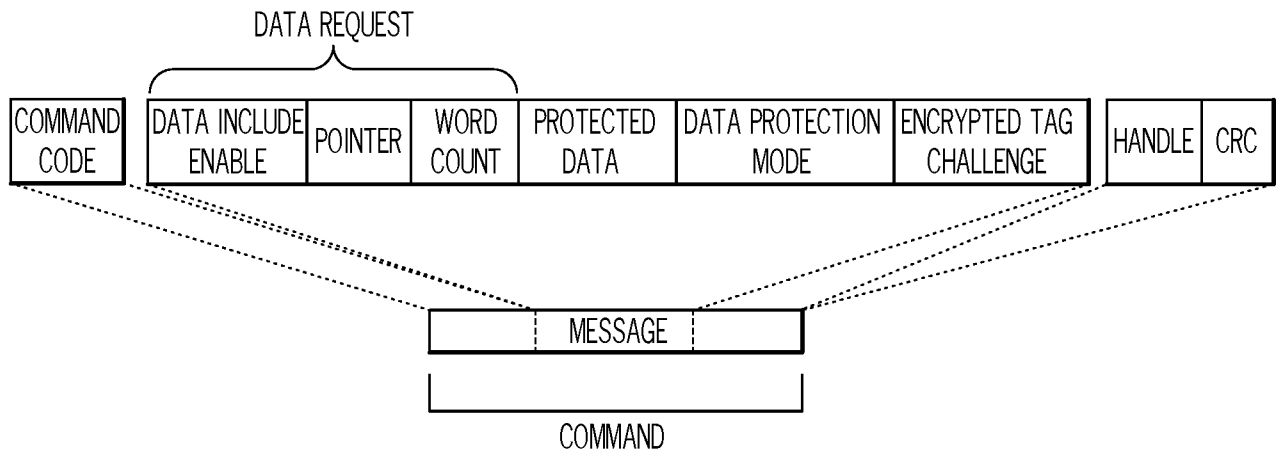


FIG. 19

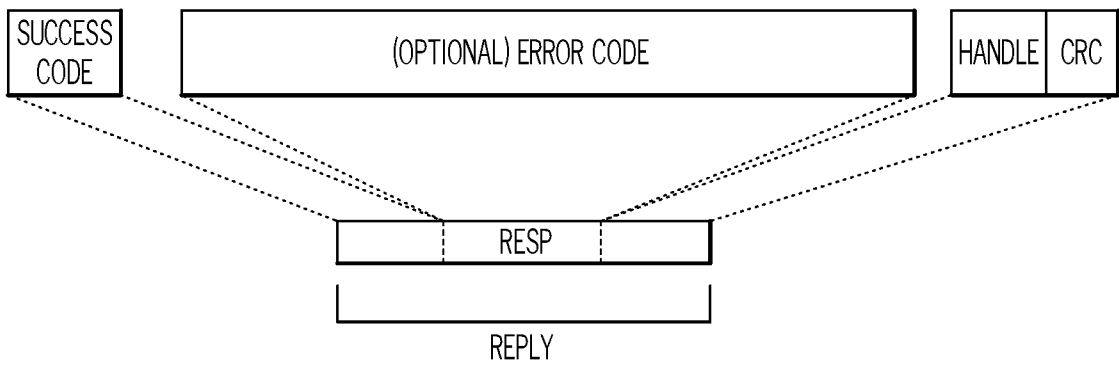


FIG. 20

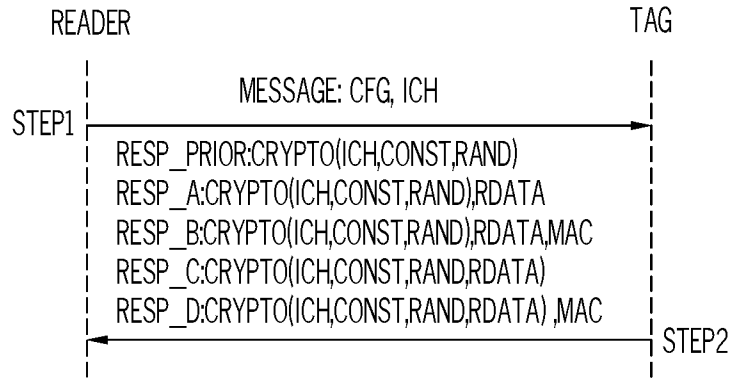


FIG. 21

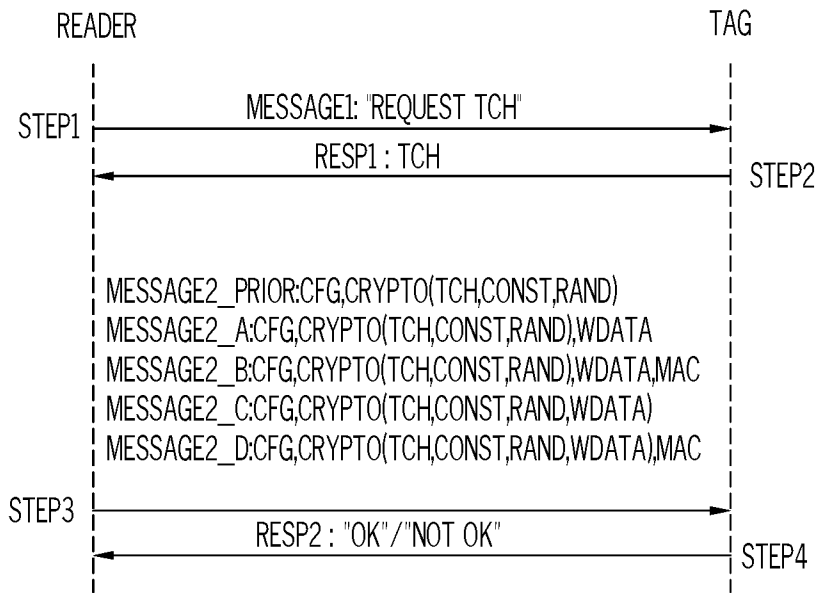


FIG. 22

INTERNATIONAL SEARCH REPORT

International application N°

PCT/IB2016/051660

A. CLASSIFICATION OF SUBJECT MATTER

IPC 2006.1 H04L9/32

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)

IPC 2006.01 H04L

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

GOOGLE PATENTS

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

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claims N°
X	WO 2011137499 A1 (BOHN JUERGEN JOSEF) 10 November 2011 (2011-11-10)	1-9
Y	page 29 lines 2-13; page 31 lines 12-20; page 40 line 22 - page 48 line 5; figures 2-3.	10-16
A	US 7450010 B1 (TC LICENSE LTD [US]) 11 November 2008 (2008-11-11)	10-16
Y	US 6842106 B2 (BATTELLE MEMORIAL INSTITUTE [US]) 11 January 2005 (2005-01-11) column 4 line 66 – column 5 line 2, claims 44-45; figure 2.	10-16

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

"A" document defining 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 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

28 June 2016

Date of mailing of the international search report

26 July 2016

Name and mailing address of the ISA/BR



INSTITUTO NACIONAL DA
PROPRIEDADE INDUSTRIAL
Rua Sao Bento n° 1, 17° andar
cep: 20090-010, Centro - Rio de Janeiro/RJ
+55 21 3037-3663

Facsimile N°:

+55 21 3037-3663

Authorized officer

Marcos Patricio dos Santos Junior

Telephone N°:

+55 21 3037-3493/3742

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application N°

PCT/IB2016/051660

Patent documents cited in search report	Publication date	Patent family members	Publication date
WO 2011137499 A1	2011-11-10	BR PI1001987 A2	2011-08-16
-----	-----	-----	-----
US 7450010 B1	2008-11-11	BR PI0710622 A2	2011-08-16
		EP 2011097 A2	2009-01-07
		MX 2008013409 A	2009-04-24
		US 2009096584 A1	2009-04-16
		US 8154405 B2	2012-04-10
		WO 2008024531 A2	2008-02-28
-----	-----	-----	-----
US 6842106 B2	2005-01-11	US 2004066278 A1	2004-04-08
		AU 2003270786 A1	2004-05-04
		CA 2500779 A1	2004-04-22
		EP 1547008 A1	2005-06-29
		MX PA05003546 A	2005-09-30
		WO 2004034321 A1	2004-04-22
-----	-----	-----	-----