CLAIMS

1. A method for sending a message from a remote server to a terminal , said remote server and said terminal sharing a secret key, said method comprising:

   i- Sending from said terminal to said remote server a first identity;

   ii- Retrieving at said remote server said first identity and retrieving said secret key based on said first identity;

   iii- At said remote server, choosing a random number and generating a second identity thanks to said first identity, said random number and said secret key;

   iv- At said remote server, generating a signature from said first identity , said message, a counter value, said random number and said secret key;

   v- At said remote server, generating a first response for said terminal, said first response being a concatenation of said message, a counter value, said signature and said random number, and ciphering said first response with said secret key and sending said first ciphered response to said terminal;

   vi- At said terminal, deciphering said first ciphered response with said secret key to obtain said first response, retrieving said message, said counter value, said signature and said random number, deriving the expected signature of said first response, verifying that said signature is equal to said expected signature and verifying that said counter value is correct, and if it is correct, derive said second identity from said first identity, said secret key and said random number.

2. The method according to claim 1, wherein if at step –ii- said remote server cannot retrieve said secret key based on said first identity, said remote server considers that a DOS attack has occurred.

3. The method according to claim 1, wherein if said first ciphered response sent to said terminal is not received by said terminal in a given time frame after having executed step –i-, said terminal increases by one the value of a counter and executes again step –i-.

4. The method according to claim 3, wherein if the message sent at step –v- is not received by said terminal and said terminal does not send a second unique identifier to said remote server, said remote server increases by one the value of said counter value, and repeats step –vi-.

5. The method according to claim 3, wherein if the message sent at step –i- is not receiving an answer from said remote server in a given time frame, said terminal increases said counter value by one and repeats step –i- with said new counter value.

6. The method according to any of the claim 1, wherein said unique identifier is sent regularly by said terminal to said remote server, on the basis of a rule sent by sent remote server to said terminal.
7. The method according to any of the claim 1, wherein said remote server is integrated in an OTA server.
8. The method according to claim 1, wherein the transport protocol between said terminal and said remote server is UDP.
9. The method according to claim 1, wherein the returned message is to inform said terminal to slow down the frequency of the requests.
10. The method according to claim 1, wherein the returned message at step –v- is to inform said terminal to increase the frequency of the requests.
11. The method according to claim 1, wherein the returned message at step –v- is to request an on board key generation.
12. The method according to claim 1, wherein the returned message at step –v- is to inform said terminal to open an HTTP communication with an OTA server.