

**CLAIMS**

1. A method for managing secure communication remotely in a network comprising:  
authorizing a gateway for communicating with a server based on a unique identifier;  
providing a credential token associated with the gateway for use in communications  
5 between the gateway and the server;  
authorizing a device for communicating with the server based on a generated key  
associated with the device, wherein the device is coupled to the gateway;  
accessing data from the device based on the key for communicating between the device  
and the server; and  
10 managing the communication between the device and the server remotely.
2. The method according to claim 1, further comprising generating the unique identifier  
comprising:  
receiving an encrypted data from the gateway;  
15 decrypting the encrypted data;  
validating and storing decrypted data; and  
generating the unique identifier based on the validated data.
3. The method according to claim 1, wherein a plurality of devices couple to the gateway.
- 20 4. The method according to claim 1, wherein the server is in communication with a  
plurality of gateway.
5. The method according to claim 1, wherein the server comprises a pool of the unique  
identifiers.  
25
6. The method according to claim 1, wherein the coupling of the device and the gateway is  
provided by physical ports or wireless communication.
7. The method according to claim 1, wherein the gateway is encrypted.

8. The method according to claim 7, further comprising creating and storing a decryption key associated with the gateway that is accessible to the server.
- 5 9. The method according to any of the preceding claims, wherein the gateway requests the server for issuance of a new credential token if the credential token is inactive.
10. The method according to claim 1, wherein the unique identifier of the gateway is generated from MAC address and product ID.
- 10 11. A system for managing secure communication remotely between a device coupled to a gateway and a server, comprising:
- the server comprising:
- 15 a processor;
- a network module configured to authorize a gateway based on a unique identifier; provide a credential token associated with the gateway that is authorized for communicating with the gateway; generate a key for the device that is authorized to communicate with the server; and manage communication between the server and a
- 20 device coupled to the gateway; and
- the gateway comprising:
- a processor;
- a communication interface for receiving and sending data from the device; and
- 25 a network module configured to provide the unique identifier for communicating with the server; receive the credential token for communicating with the server; and authorize the device for communicating with the server;
- wherein the server, the gateway, connects to the device, obtains data from the device
- 30 and sends the data to the server via the communication interface to manage the data received from the device remotely.
12. The system according to claim 11, wherein the server comprises a pool of the unique identifiers.

13. The system according to claim 11, wherein the server is in communication with a plurality of gateway.
- 5 14. The system according to claim 11, wherein the device is coupled to the gateway by physical ports or wireless communication.
15. The system according to claim 11, wherein the gateway is encrypted.
- 10 16. The system according to claim 15, wherein the gateway is configured to create and store a decryption key that is accessible to the server device.
17. The system according to claim 11, wherein the gateway requests the server for issuance of a new credential token if the credential token is inactive.
- 15 18. The system according to claim 11 or 12, wherein the unique identifier of the gateway is generated from MAC address and product ID.
19. The system according to claim 11, wherein the system is configured for adopting and  
20 integrating by the server and/or the one or more devices.
20. The system according to claim 19, wherein the system is configured to provide centralized management of the one or more devices remotely.
- 25 21. The system according to claim 11, further comprising a network communication means configured to allow transmission between the server and the device.