10 Points on Casambi Security

1. WiFi is a Problem

If WiFi is needed for the normal operation of a lighting control solution, there is something fundamentally wrong with that lighting control solution's architecture.

Besides bringing problems in performance, cost, power consumption and user experience, WiFi adds a high vulnerability for cyber attacks and puts the system's security at risk.

Casambi uses Bluetooth Low Energy and a tailored mesh network for normal operation, no WiFi connection is needed.

2. The Casambi Network

The Casambi network (communication from mobile devices to Casambi units and Casambi units to the cloud and server) is an own, closed network. Local building networks cannot be accessed.

3. The Casambi Cloud

Log In and Password are needed that allows an access token* to a local "Bluetooth network".

Passwords are stored using one-way hash algorithms. With an access token only a local network can be accessed.

* ***Access token*** *is a session identifier that allows a guest or a manager level access to the network for one mobile device. When network passwords are changed all the existing access tokens are invalidated.*

CASAMBI

4. Servers

Casambi uses Linux servers protected with industry best practices. All communication is done via HTTPS*.

Servers are firewalled and monitored 24/7. They are kept up to date with security updates, access only by limited personnel and the stored information is encrypted.

**__HTTPS__ stands for Hyper Text Transport Protocol Secure and is a trusted end-to-end communication process. HTTPS prevents hackers from sniffing out passwords and hijack user accounts.*

Example: HTTPS commonly used by banks and other websites handling money.

5. Communication between a mobile device and a Casambi unit

Each request is signed with a unique authentication to verify that user has privileges to perform operation, i.e. changing configuration or controlling fixtures.

Firmware updates are signed with authentication, units only accepts firmware that originates from Casambi.

6. Communication between two Casambi units

Casambi units use industry strength security measures* for protection against eaves-dropping and common security attacks. Each packet is encrypted and signed; units will also perform bi-directional authentication between all other nearby units on same network. Each packet contains rolling code that protects against replay attacks (listen and re-send).

** The industry strength cryptographic toolbox that are in use are 128-bit AES for message encryption and AES-CMAC for message authentication.*

7. Gateway Communication

The gateway access is through the Casambi cloud. All communication is HTTPS*.

8. Sharing Settings

Please remember to set your network sharing settings on a suitable level. Please keep the administrator device and the passwords as your personal knowledge.

Not Shared: The Network is only stored on the device the network has been created with. Other devices cannot access the network.

Administrator Only: The Network is discovered and accessed only with an administrator e-mail and password (chosen at the stage of creating the network).

Password Protected: Other devices can access the network with a visitor password. Modifications require an administrator password.

Open: Other devices can access the network without any password. Modifications require an administrator password.

9. Worse case scenario with Casambi

In case, against all odds, a Casambi network would be hacked, the only thing a hacker can do after such an intrusion- is to control the lighting.

10. Smart and connected

The ideal network architecture includes smart devices, that are smart on their own and are connected only when needed- instead of needing a WiFi connection to be smart. **Casambi is truly Smart & Connected**.