CASAMBI

May 2020

Casambi Security

Encryption:

- 128-bit AES: Symmetric encryption cipher.
- AES-CMAC: Message authentication algorithm for data integrity.
- ECDH: Elliptic curve key exchange.
- ECDSA: Elliptic curve digital signature algorithm.
- Full encryption between mobile device and units. New encryption key for each connection, derived with ECDH.
- 10 changeable passwords.

Preventions:

- Prevention of replay attacks: using rolling codes for packets, and two-way authentication between units to validate initial rolling codes.
- Prevention of eavesdropping: fully encrypted communication. Unit-to-unit communication is even impossible from network administrators to decrypt.
- Prevention of man-in-the-middle attack: two-way authentication between mobile device and unit, and unit-to-unit.
- Prevention of trash-can attack: mobile device verifies the authenticity of the unit before it is added to network.
- Prevention of tampering: strong message integrity checks

Cloud security:

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

The cloud requires Log In and Password, 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.

Mobile device to Cloud communication:

The connection from a mobile device to the cloud is secured by TLS (Transport Layer Security).

All communications are done via HTTPS (Hyper Text Transport Protocol Secure) which is a trusted end-to-end communication process. Prevents hackers from sniffing out passwords and hijacking user accounts.

Casambi Technologies Oy. Alberga Business Park. Bertel Jungin Aukio 1 E. 02600 Espoo Finland

Topology:

Self-healing Bluetooth Low Energy mesh (BLE). No single point of failure: no single critical element that stores the information needed for the proper functioning of the network or part of it. If a device fails, the signal flow automatically reroutes through other devices ("self-healing"), which increases reliability through multiple nodes and redundancy of nodes.

Every Casambi device is independent and has a backup of the entire network (therefore it's possible to recover the backup of any device with a single tap on the mobile device). Speeds up the communication and makes the communication more robust.

BLE avoids conflicts with other 2,4 Gz band wireless technologies, as WIFI, due to the hopping technology. BLE works in dynamic channels instead fix channels.

Every Casambi device acts as an amplifier (30m range indoor).

Casambi network operates also without an internet connection.

Network accessibility:

Four different levels

- **Not shared:** The network (Casambi devices) is not visible and can only be accessed with the username and password.
- **Password protected:** The network is visible with Casambi app but the password is needed to access it. Possible to use and edit the network, *except sharing settings.*
- **Open**: The network is visible with Casambi app and anyone can access it with the app. Possible to use and edit the network including sharing settings.
- **Admin**: Administrator, all rights.

Up to ten different passwords can be added.

Possibility to allow/deny firmware updates.

Possibility to allow network backup automatically, every time is edited, periodically or manually. Backups can be restored from the Casambi Cloud.

Possibility to lock the Casambi units.