BlipTrack WiFi/BLE/Bluetooth Sensor Anonymisation Procedure

Using sensors to detect mobile devices for queue and flow analysis may raise concerns about data security and personal data protection. We take pride in anonymising all collected data, and we go to great lengths to maintain a high standard of protective measures.

Detecting Devices

The BlipTrack sensors work by detecting WiFi/BLE/ Bluetooth-enabled devices, like phones, headphones and smartwatches and more.

As the device passes a sensor, the unique device ID (MAC address) is timestamped and encrypted.

Through re-identification, as the device passes multiple sensors, the system measures travel times and movement patterns.

One-way Hash and SSL Encryption

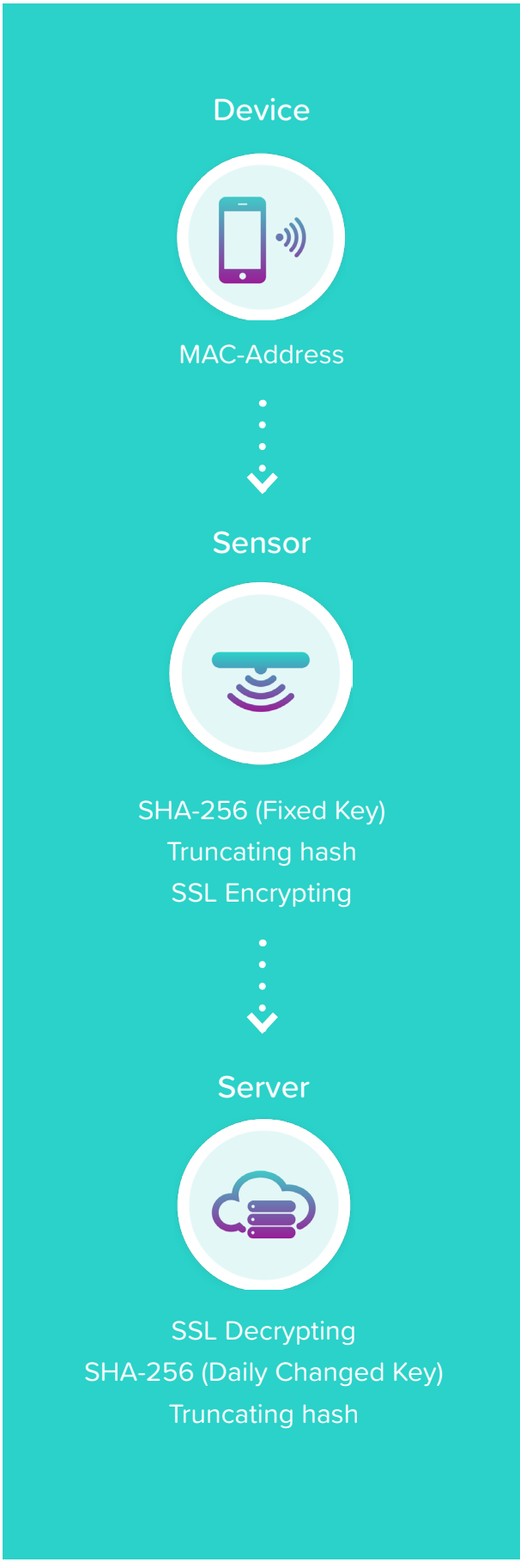
Each sensor has an SHA-256 anonymisation algorithm, which generates a one-way hash code of the detected MAC address of a mobile device before it is forwarded to the server.

As only part of the hash code is transmitted, it is impossible to relate or revert hash codes back to real MAC addresses.

Communications between the sensor and the server are encrypted using SSL.

Re-hashing

Before storage, the hashed MAC addresses are hashed once again, using the SHA-256 algorithm with a random SALT key, which is changed daily at a predefined time. The SALT is volatile, meaning it is not persisted in any storage, and cannot be restored in any way once the SALT is updated. The second hashing also prevents any identification of returning devices.



BLIP Systems A/S, Haekken 2, 9310 Vodskov, Denmark -
+45 98 25 82 00 - sales@blipsystems.com - wwww.blipsystems.com