LinkThru Security Policy

LinkThru Security

LinkThru is hosted by SPICA Technologies Ltd on their Devicepoint® Application Framework.

This overview details the Security Model at and between each of the solution layers from devices at the Edge of the network, through to Cloud platforms and to User Dashboards.

Devicepoint® - Security Principles

Customer Information - No information about the Customer is transmitted between device and Spica Devicepoint® Platform or held in network provider clouds.

Device to Customer Link - This is held solely in the Devicepoint® Platform.

Security Layers - Security exists at every layer and between each layer: Device, Router, Base Station, Cloud and End User.

Platform - Devicepoint® Platform is hosted on security accredited Cloud Platforms (AWS or IBM).

Access Control - Role-based user access provisioning ensures only authorised users have appropriate access to data.

Encryption - Payload is encrypted with a symmetric private key.

Devicepoint® – Cloud Platform Security

Single Tenanted Virtual Machine - Application Instance and Database can be provisioned to hold only a single client's data.

Devicepoint® Platform Web Access - HTTPS -Username / Password logon. Individual Users have Role-based access to functionality. Roles/Users can be granted access/control to different levels of the Devicepoint® hierarchy.

Devicepoint® to SIGFOX Cloud Platforms (APIs) - SSL/HTTPS

Devicepoint® - SIGFOX Security Layers

Devices - Unique ID Per Device, PAC Code Registration. AES Based Private Key Authentication for each device. Authentication credential ONLY checked by SIGFOX Cloud

Device to Base Station - Ultra Narrow Band (UNB) signal with Native Random Frequency Hopping. Gives high resistance to Interference and Jamming

Base Station - Locations Confidential, Physical Security in place, Base Stations have Firewall

Base Station to SIGFOX Cloud - VPN Connection

SIGFOX Backend - Replay Attack Detection and Notification, Brute Force Attack Detection and Notification, Unexpected Base Station Reception Detection and Notification, Software Defined Radio (SDR) and Software Defined Network (SDN) - Physical radio "fingerprint" can be checked

Data Lifecycle Management

All customer instances of Devicepoint® have daily back-ups taken. The back-up consists of a full copy of the database image for the Devicepoint® instance. A rolling set of back-up images is kept for the previous 7 days.

In the event of an emergency an entire customer instance of the system can be recreated (from a brand-new server instance if required), the latest (or earlier) database instance can be restored to this recovered/rebuilt instance, and the customer system will be operational again. For most sensors connected to the system, any data lost during the outage will be recovered from sensor gateways.