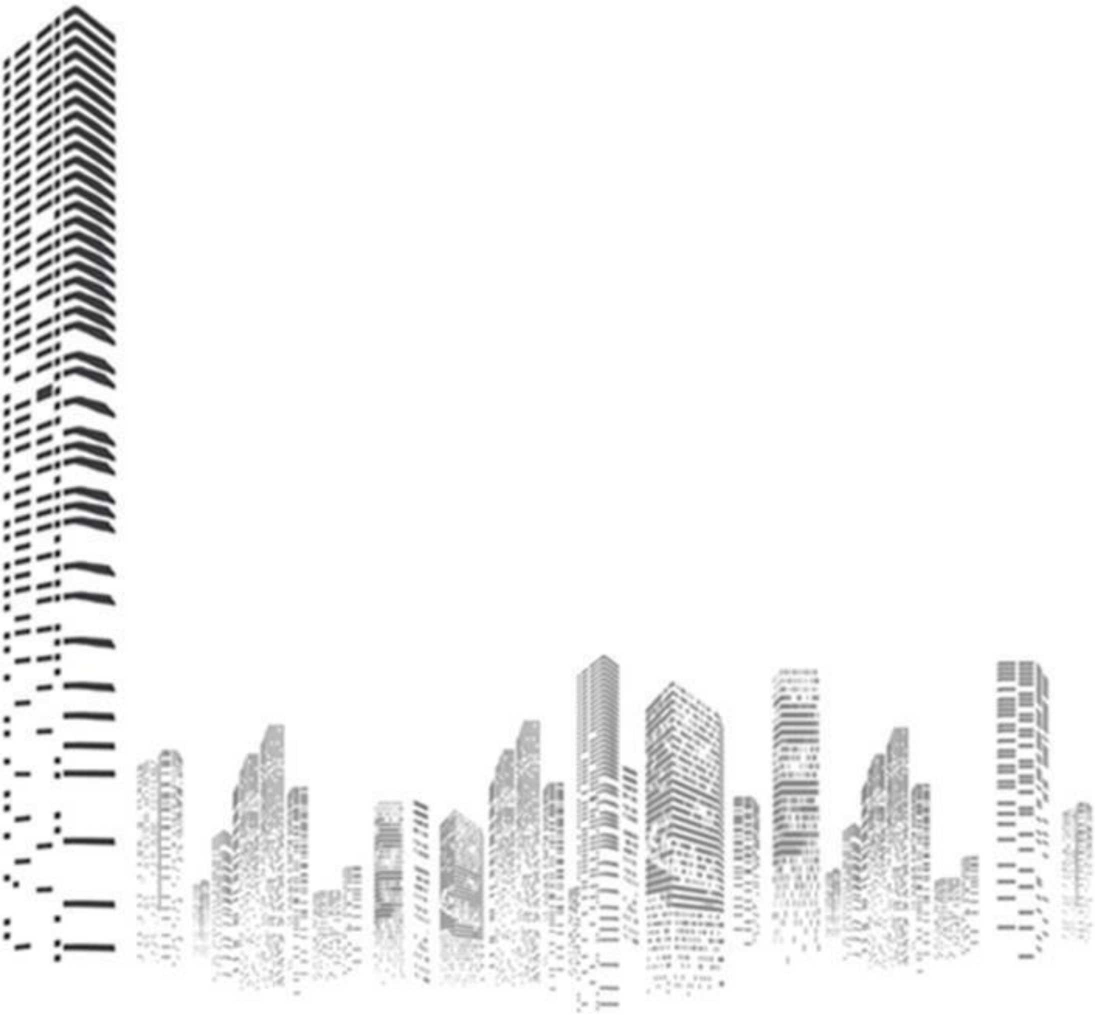
Rev 2

Monitoring Service Security & Data Privacy



Contents

Revision History

Author	Date	Notes	Rev
LC	2/2/2018	First Draft	0.1
LC TO	28/3/2018	Proof Read Draft	0.2
LC TO NJ	29/3/2018	First issue	1.0
TO	6/6/2018	Omitted Tosibox and 4G, MC renamed to HCG	1.0a
TO	19/7/2018	Re-Included Tosibox	2.0

OJ	22/02/2021	Update latest security information and feature improvements	3.0

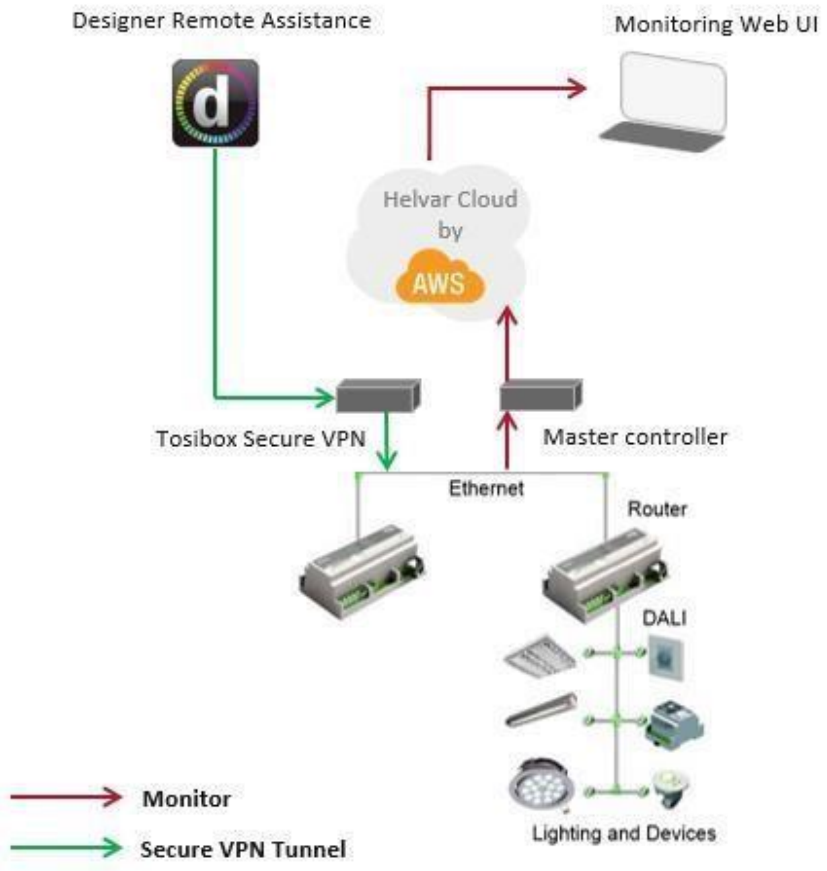
Introduction

The Helvar monitoring and maintenance service enables its customers to have visibility regarding system health, building occupancy, light level status, and emergency lighting test reports. In addition it provides remote assistance and support of their lighting control system.

The service is a cloud based system that also depends on being able to connect to the on premise lighting control system to facilitate the collection of data and communication transmissions between the service and the control system.

This document provides a comprehensive overview related to the security and integrity of the solution.

System Overview



Helvar services are enabled by connecting its lighting control system (Helvar routers) to a Cloud Gateway, then the Cloud Gateway to the Helvar Cloud. The role of the routers is to provide control of the DALI lighting system which consists of luminaires, presence detectors, push buttons etc. The role of the Cloud Gateway is to securely get and send the data collected by the routers to the Helvar cloud infrastructure and also to receive communications from the Helvar Cloud. The Helvar Cloud is where the data is securely stored and processed.

Local and Internet Connectivity

The Cloud Gateway can use standard Ethernet and Wifi for local network communication and requires certain firewall permissions to enable connectivity to the internet and the Helvar Cloud. In order to connect to the Helvar routers the Cloud Gateway uses Ethernet which can either be realised using layer 2 or layer 3 networks. When deploying to a layer 3 network, Helvar recommends that the router network be isolated and securely locked down using MAC addresses of the network adapters of the routers and Cloud Gateway.

Cloud Gateway security

The Cloud Gateway is shipped pre-configured. It implies that no password is stored locally and therefore if an unauthorized entity would gain access to the Cloud Gateway, they would not be able to access the data in the Helvar Cloud.

The Cloud Gateway is always mapped to a unique site and can only access and collect data of the associated site.

Between On Premise and Cloud

The system uses a combination of MQTT and HTTPS to communicate between the Cloud Gateway and the Helvar Cloud. These communications are secured by leveraging TLS 1.2 at the transport layer. The cipher suite used for TLS is ECDHE-ECDSA-AES128GCM-SHA256. For HTTP communications 'AWS signature version 4' is used for authentication between Cloud Gateway and Helvar Cloud.

External Access

The services part comprises of both a web browser interface and an API interface. Access to both requires authentication which is handled by AWS. The Helvar Cloud provide the ability to sign up with a password and MFA to ensure that it authenticates access securely.

Once authenticated, users must have the right authorization to access certain features and data that have been assigned to them. The Helvar Cloud allows for specific site and secondary sub-site space access. Additionally, there are certain user defined roles that can be used to further restrict or grant the necessary access to data and service features.

Security, Data and Privacy

Driving principles

1. **Encryption in Transit:** All data transferred is systematically encrypted.
2. **Encryption at Rest:** All data stored with the Helvar Cloud is encrypted.
3. **Least privilege:** Access to the data is only provide to Helvar employees that require it.
4. **Authentication:** Only authenticated entities and persons are eligible to access Helvar data and services.
5. **Pre-configuration:** Helvar pre-configures every Cloud Gateway so that it can only access, collect, store and send data for the site it is purposely destined to.
6. **Authorization** is "white listed" by default, meaning that no person nor entity would be eligible to access the data and service by default.

Data ownership

Helvar is committed into making no ownership claim over the data it collects. Helvar reserves the right to use the data to optimize the operation of the building in relation to the Helvar Service offering.

Data transfer

The data transfer between the client and cloud is secured by using MQTT and HTTPS protocol. The only eligible data destination is the Helvar cloud infrastructure. To ensure data transfer integrity from the Cloud Gateway to the Helvar cloud, all communication channels authenticated before data is transmitted.

Data privacy

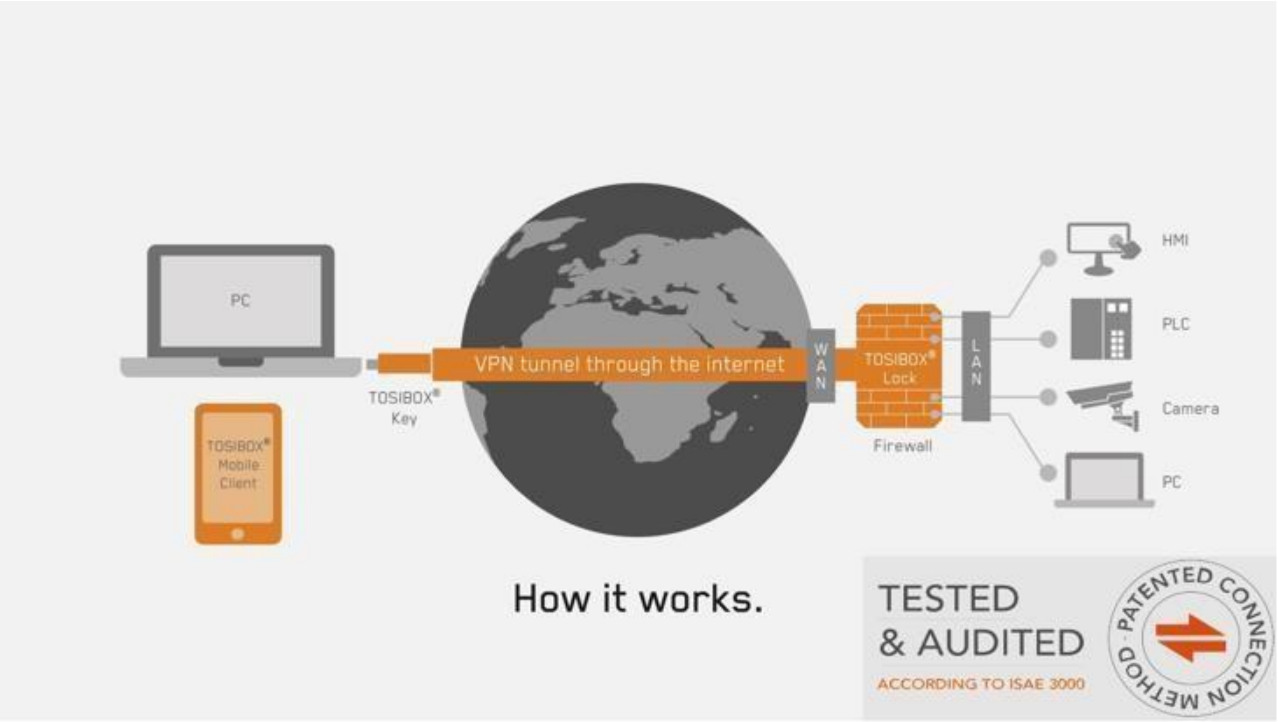
Helvar is committed not to collect, store or use data that would directly or indirectly permit the authentication of a person in a building. All data collected is anonymous and cannot be directly traced back to individuals.

Data Storage Location: The AWS servers Helvar use are in Ireland ensuring that all data stays in the EU.

Remote Assistance

Via VPN Tunneling

Helvar’s secure VPN access uses the TOSIBOX® solution which is third party tested and audited in accordance with the ISAE3000 Assurance Standard. This method requires authorization from the on-site network administration team.



What makes TOSIBOX® so secure?

Security audited by a third party

The information security of TOSIBOX® products, services, and operations are officially audited. The security audit was conducted by a global independent company according to the ISAE3000 Assurance Standard and the controls and content of the audit were based on the ISO 27001:2013 standard and the OpenSAMM Software Assurance Maturity Model. See the news article and press release for more information.

Secure by design

Trust is based on *physical serialization* – This unique process matches together, cryptographically, the physical TOSIBOX® devices, creating a trust relationship between them.

TOSIBOX® use *two-factor authentication* (2FA) in our products. It means that there are two different things required for the user to authenticate and get access:

1. Something that the user has – the physical TOSIBOX® Key or a mobile device
2. Something that the user knows – the password

End-to-end encryption – The VPN connection is established directly between the TOSIBOX® devices and the data can be decrypted only at the connection end points (devices). Nobody – not even TOSIBOX® Oy – can decrypt the data in between.

Thanks to Tosibox's *patented connection method,* the connection can be established even when both parties are behind firewalls or NATs. As a result, in TOSIBOX® devices there are no services that would be all the time listening or exposed to the Internet.

TOSIBOX® products have no backdoors and Tosibox Oy does NOT retain any private keys or passwords for the products.

Tosibox products use *industry standard* and use *proven technologies* such as the RSA cryptosystem, AES encryption, Diffie–Hellman key exchange and TLS sessions.

Via Teamviewer

In order the remotely support issues regarding the HCG Helvar also utilises TeamViewer. This method requires authorization from the on-site network administration team. Further information regarding the use of Teamviewer can be provided on request. If this is not granted but the Tosibox solution is authorized then Teamviewer can still be utilized by using the Tosibox VPN connection and enabling LAN connections.

END