Rev 1.0

Monitoring & Maintenance 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

Introduction

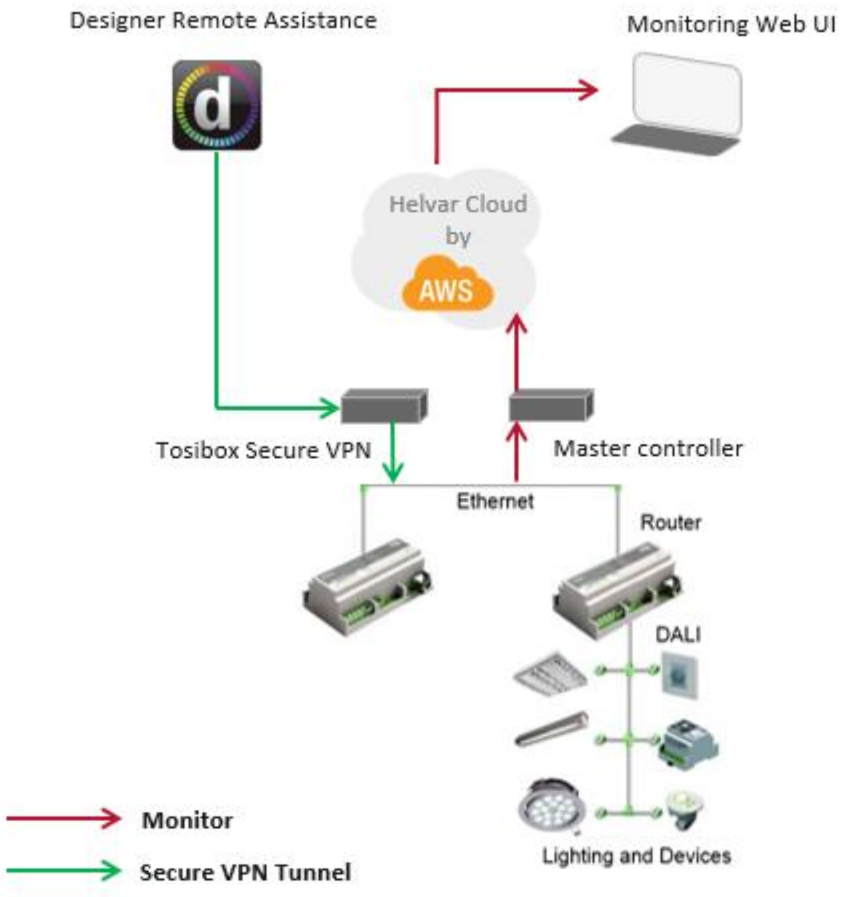
The Helvar monitoring service enables its customers to have real-time system health check visibility and remote assistance of their lighting control system.

The service is a cloud based system which comprises of both a web browser interface and an API interface. The APIs are meant to add flexibility for specific service creation.

The access to the web interface and the APIs are both encrypted and authenticated, preventing unauthorized parties to access or to read data.

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 Master Controller, then the Master Controller to the Helvar Cloud infrastructure. The role of the routers is to provide control of the DALI lighting system and consist for luminaires, presence detectors, push buttons etc. The role of the Master Controller is to securely get and send the data collected by the router to the Helvar cloud infrastructure. The Helvar cloud based infrastructure is where the data is securely stored and processed.

The protocol used to communicate between the Master Controller and the cloud is MQTT which is secured by leveraging TLS 1.2 at the transport layer. The cipher suite used for TLS is ECDHE-ECDSA-AES128-GCM-SHA256. For authentication between Master Controller and cloud we use AWS signature version 4.

The Master Controller can use standard Ethernet, wireless or 3/4G networks for communication.

Only authenticated users of a particular site can gain access to its data.

Security, Data and Privacy

Driving principles

1. **Pre-configuration:** Helvar pre-configures every Master Controller so that it can only access, collect, store and send data for the site it is purposely destined to.
2. **Separation:** The Helvar service is not dependent on the building network infrastructure. It can operate separately from it, using a 3/4G network.
3. **Encryption:** All data transferred is systematically encrypted, using TLS 1.2
4. **Data integrity:** In addition to the encryption, Helvar leverages from the commercial grade solution AWS (Amazon Web Services) to ensure data integrity for its cloud based infrastructure.
5. **Authentication:** Only authenticated entities and persons are eligible to access Helvar data and services. The authentication is “white listed” by default, meaning that no person nor entity would be eligible to access the data and service by default. The authentication mention is based on AWS signature version 4.

Master Controller security

The Master Controller is shipped pre-configured. It implies that no password is locally stored and even if an unauthorized entity would gain access to the Master Controller, they would not be able to access the data.

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

The Master Controller is only used for collecting data from the Lighting Control system and cannot affect the operation of the system.

Data transfer

The data transfer between the client and cloud is secured by using HTTPS protocol. The only eligible data destination is the Helvar cloud infrastructure. To ensure data transfer integrity from the Master Controller to The Helvar cloud, all transactions and involved parties are systematically 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 traced back to individuals

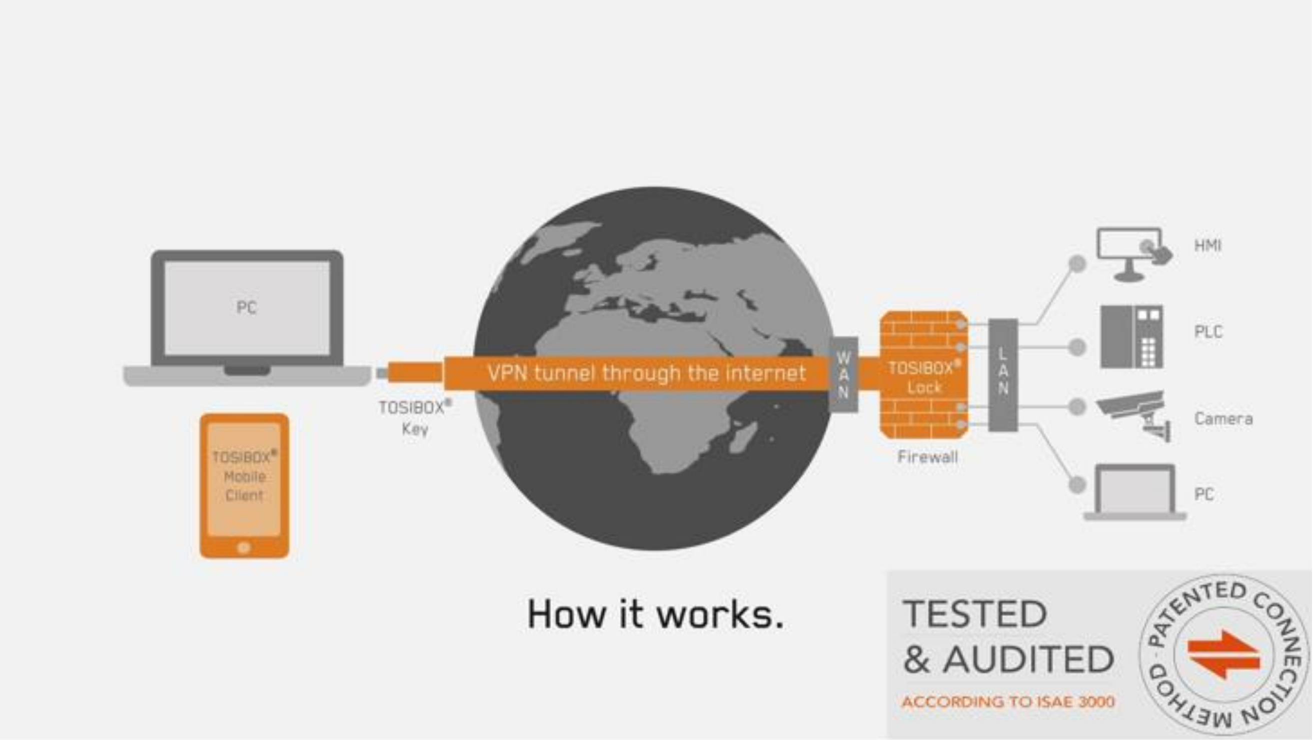
Data Storage Location: The AWS servers Helvar use are in Ireland ensuring that all data stays in the EU.

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.

VPN Tunneling for Remote Assistance

Helvar's secure VPN access uses the TOSIBOX® solution which is third party tested and audited in accordance with the ISAE3000 Assurance Standard.



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

END