EYESEAL

Technical Reference Guide

TEMPEST

Table of Contents

Introduction	3
Answers to your specific questions	4
EyeSeal at a glance	5
Technical specifications	6
Fixing, sealing, and locking the device to the container	7
Data tracking	8
Connectivity & data transmission	10
Current phase 2 system architecture diagram	11
Surrounding infrastructure	12
Track record	13

Introduction

Thank you for your interest in our smart seals. We believe our innovative technology can revolutionize container security and integrity in multiple industries.

This document provides comprehensive insights into our company, product specifications, and applications.

We will cover the design, attachment methods, sealing mechanism, data collection capabilities, location determination, battery life, data security, market availability, and additional valuable information.

We aim to foster a fruitful partnership and look forward to your feedback.

Answers to your specific questions

We thought it might be useful to first provide a few short answers to the questions you shared with us.

Shape and volume of the smart seal

The EyeSeal device is compact and lightweight, offering convenience and portability. For detailed information, please refer to page 6.

Method of fixing to the container

Devices are easily installed inside shipping containers by hanging them from the beam above the doors using magnets or a strong adhesive. They establish direct physical contact with both container doors. A step-by-step description of the installation process can be found on page 7.

Sealing, locking

After fixing the EyeSeal device inside the container and activating it, the sealing is accomplished simply by closing both doors. A detailed description of this process can be found on page 7.

Data collected (location, sealing status, movement, acceleration,...)

Eyeseal monitors multiple data points, including door breaches, light variations, internal temperature, humidity, and geographic location. A comprehensive overview of sensor functionality can be found on page 8.

Method of location determination and accuracy

EyeSeal utilizes triangulation with the assistance of cell towers to accurately determine its position. This data is seamlessly captured and integrated into EyeTrack, which is EyeSeal's proprietary data platform. For more detailed information, please refer to page 10.

Method of sending the data, battery and autonomy

EyeSeal ensures the highest level of data security by implementing military-grade encryption for all the data it transmits to the EyeTrack platform. The device's battery is designed to remain operational for a minimum of 120 days, assuming standard alert intervals are configured.

The actual battery life will vary based on the user's preferred frequency of alerts. For detailed information regarding the batteries, please refer to page #. Additionally, comprehensive details about data handling can be found on pages # to 10.

On the platform and data: configurability and security

For detailed information about the configurability of the device, please refer to page 11.

Moreover, EyeSeal provides the capability to share data with other platforms through APIs, allowing seamless integration and interoperability.

Track record

EyeSeal devices have been monitoring cargo shipments since 2018, passing through more than 75 countries. The device has also been tested and approved during the Gateway2Britain pilot project.

Please refer to page 13 for more detailed information about EyeSeal's track record.

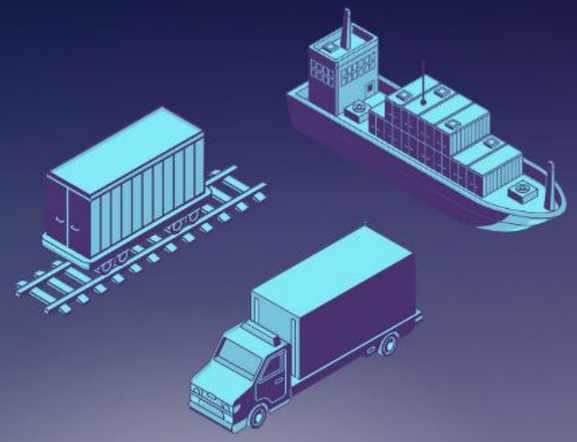
EyeSeal at a glance

EyeSeal device installation → Constant monitoring during entire voyage → Cargo arrives at destination

The EyeSeal device is installed inside the shipping container and activated

EyeSeal regular updates and alerts are encrypted and transmitted via 3G GSM networks

All vector, full stack endpoint security agent managed by an AI engine in real time .



Breach alerts can trigger drone deployment (optional)

Upon arrival at final destination EyeSeal generates a full detailed forensic report of the entire voyage.

DIRECT DATA

- Location tracking
- Breach and door monitoring
- Advanced anti-hacking protection

- Light detection
- Temperature monitoring
- Humidity monitoring

Technical Specifications

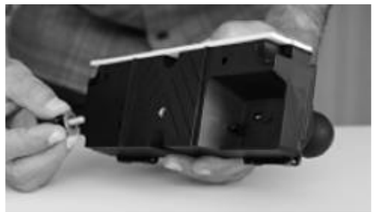
Dimensions of the EyeSeal unit	
Height	81.1mm
Width	216.8mm
Depth	47.8mm
Weight	15.2 ounces (430 grams)
Housing Material	UL 940-V0 flame retardant plastic
Rubber door detector boots	Height: 78.7 mm Width: 52.7mm Depth: 50 mm

Battery specifications	
Power	9.6Ahr
Battery Type	High-capacity internal Lithium Thionyl Chloride
Autonomy	At least 120 days for standard signal configuration
Operating Temperature	-25°C to +70°C
Storage Temperature	-40°C to +85°C
Environmental Rating	IP67
UN Battery Code	3091

Cellular connectivity	
2G	GSM/GPRS, Quad band 850/900/1800/1900 MHz
3G	UMTS/HSPA+, Global, 800/850/900/AWS/ 1700/1900/2100MHz
4G	LTE CatM1(Rel.14), LTE Cat NB2 (Rel.14) w/EGPRS (2G Fallback)
Countries with coverage	170

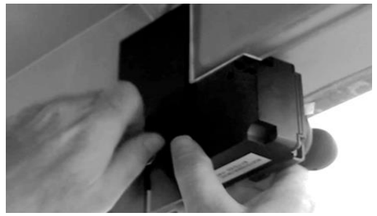
Other specifications	
Export Control Classification	# 5A991.g
HSN Code (Harmonized Shipping Code)	8526.91.0040
Dangerous Goods designation	Type 9

Fixing, sealing and locking the device to the container



Thread the bolt with the washer to the back of the unit (two to three rotations only)

Align the unit with the alignment tool, making sure the bolt and the washer are loose enough to allow the unit slide up the slot. Different mounting tools are available for different types of containers and trailers



Push the unit upward until the magnet/adhesive makes full contact with the frame and tighten the bolt.

Once the unit has been fastened to the top frame, remove the activation slip to initiate the device. Alternatively, the device can also be activated before installation.

Close the left door. Make sure that the right “rubber boot” on the unit is flush with the left door frame. The unit is now correctly installed and the containers doors can be sealed for transport.

Data Tracking

The Eye-Seal Internal Container Breach Detector is a comprehensive solution that offers unparalleled security for cargo during shipping.

One of its key features is the Eye-Track user interface platform, which enables stakeholders to track the container's location and status in real-time, regardless of whether it's being transported by truck, rail, sea, or a combination of the three.

Using the Eye-Track platform, stakeholders can access and monitor extensive data captured and displayed by the Unit, including door position (open or closed), internal light values, temperature, humidity, and dew point.

By default, the Unit records this data every six hours during the entire voyage, and it's displayed as an in-route "Scheduled Report" for stakeholders to view.

In the event of any deviation from the container's monitored data, the Eye-Track platform immediately issues an "Alert" to designated users, providing them with a date and time stamp, as well as location information. This ensures that stakeholders are notified promptly of any potential issues with the cargo, allowing them to take swift action to mitigate the situation.

The Eye-Track platform offers an ongoing full voyage "Report" that includes all the unit data collected from the origin point to the final destination. This report can be shared with all stakeholders in the supply chain, providing them with comprehensive and accurate information about the cargo's journey.

With its advanced technology, real-time data tracking, and immediate alert system, stakeholders can rest assured that their cargo is secure and protected throughout the entire journey.

Data Tracking

Our UI will allow you to provide access to as many individuals in your logistics chain that you wish to include. Including Security, Forwarders, Insurance, Consignee, Transport managers. Anyone that you allow access to the UI now has access to these reports and details.

Your team will have full details for the following key points:

- Date and time door originally closed after loading.
- Full history of container condition from loading unit
- inspection at warehouse exit.
- Exit Message prior to leaving the warehouse including full history from loading.
- Scheduled messages every six hours with full date time, and location stamp (including environmental parameters).
- Immediate alerts upon both authorized and unauthorized breaches.
- If the 6 Hour schedule is maintained – the Eye-Seal can provide this coverage for 120 days internationally. The device parameters and interval is established when the device is ordered.

With these key date, time, and locations stamps combined with the actions observed by the sensors, Law Enforcement and Insurance can define a specific timeline and location.

The Custody of the container will be known and thus responsibility properly assigned.

When thefts are undetected for several days, weeks or months, the cargo has passed through the hands of several players along perhaps international borders and jurisdictions. At this point it is nearly impossible to identify the Custodian of the Cargo when the said breach occurred.

However, In the Maritime field, a six hour window is a short time frame to properly make an exchange of Custody. The Custodian will be identified with the Time and Date Stamp.

Connectivity & Data Transmission

The diagram on the right illustrates the data exchange process between the EyeSeal device and the Server.

The improved architecture incorporates a CQRS+ES (Command Query Responsibility Segregation and Event Sourcing) system, where events from the devices are collected and stored in an immutable event journal.

This journal serves as the basis for projecting device status updates into an SQL server, powering the web site. This decouples the TCP endpoint from the web site and enables system scalability. Additionally, it provides an auditable trail of events, allowing for evidence of a device's status at any given moment.

At the beginning of each communication session, a unique 320-bit session key is generated by the Server. This session key is transmitted to the Device using XXTEA encryption and a 128-bit key, which is generated in the factory and known only to the device and the Server.

All transmitted data is combined with the 320-bit session key, and the resulting data stream is used to create a SHA-1 Cryptographic Hash. This hash is sent along with the data to enable the Server to validate the transmitted data.

The key used for XXTEA encryption is stored in protected memory within the device, safeguarded by an 80-bit access code. In case of an incorrect access code, the memory is erased to prevent unauthorized access.

If tampering is suspected, the Eye-Seal engineering team can recover the non-volatile data log stored on the device.

Encrypted communication protocol between the EyeSeal device and the EyeTrack data server

Device Sends identity to Server

Server replies with XXTEA encrypted 320-bit session key

Device replies with SHA-1 hash of pre-agreed data

Server requests status dump

Device replies with Jason formatted data and SHA-1 hash Jason data + session key

Server acknowledges receipt of data

Server sends disconnect command

Device acknowledges and disconnects

Current phase 2 system architecture diagram

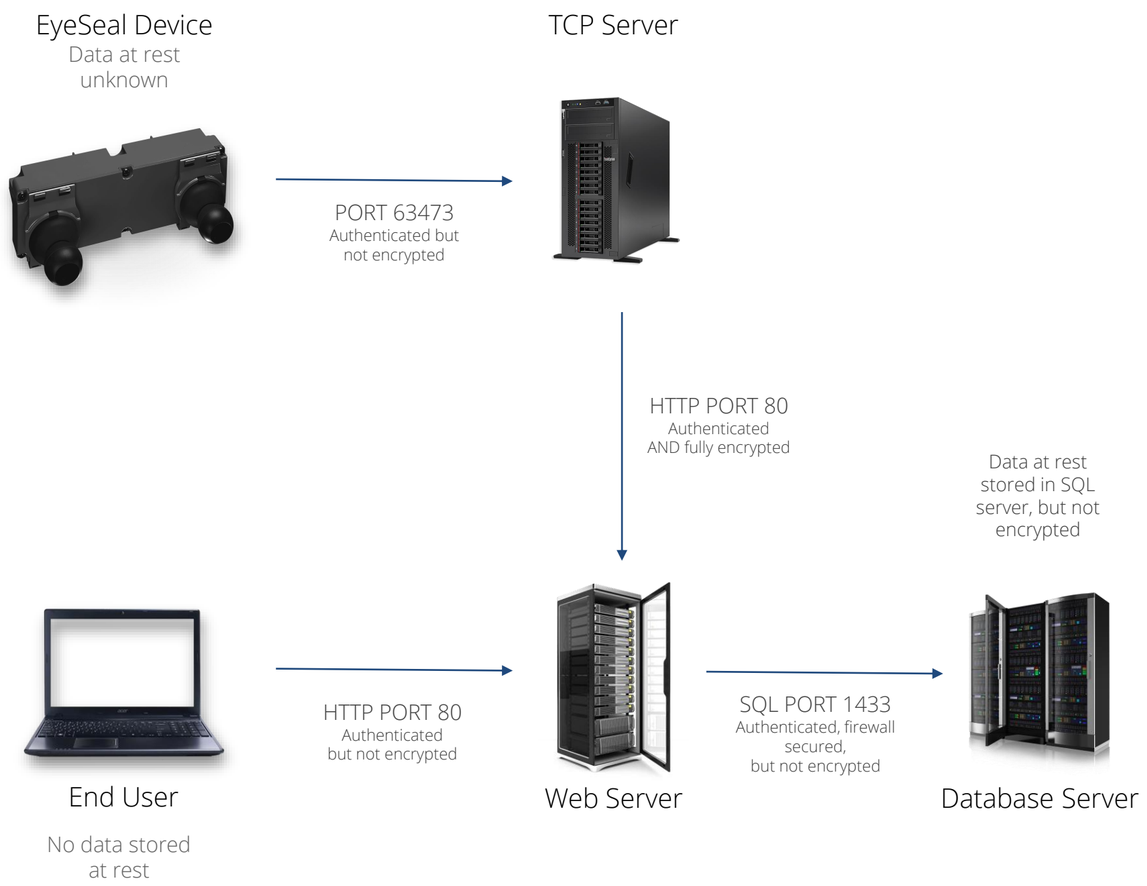
DiscoverTec is currently designing the architecture for Phase III implementation, with a proposed plan to adopt a CQRS+ES (Command Query Responsibility Segregation and Event Sourcing) system. In this system, events from the devices will be collected and stored in an immutable event journal.

Subsequently, the journal will be utilized to project device status updates into an SQL server, empowering the web site. This approach logically separates the TCP endpoint from the web site, facilitating easier scalability. Moreover, it provides a verifiable audit trail of events, ensuring the ability to demonstrate a device's status at any given moment, even in legal proceedings.

DiscoverTec's High-Availability infrastructure serves as a strong foundation to meet the performance and reliability requirements of customer applications. High availability, in this context, refers to the absence of human intervention needed to restore operation in complex systems. DiscoverTec achieves high availability without compromising performance through the implementation of active redundancy.

The design incorporates multiple identical items equipped with failure detection mechanisms. In case of failure, the system automatically reconfigures itself by employing a voting scheme to bypass the failed components.

Additionally, DiscoverTec's certified engineers have hardened and scaled the infrastructure to be secure and dynamic. The infrastructure is designed to eliminate chokepoints and bottlenecks, ensuring smooth operations. It can seamlessly scale to meet the evolving needs of businesses, adapting to emerging requirements.



Surrounding infrastructure

DiscoverTec prioritizes maximum reliability and performance by strategically deploying their systems in two geographically dispersed data centers. These data centers boast redundant power network infrastructure and state-of-the-art environmental controls.

To maintain top-notch security, DiscoverTec employs sophisticated systems for Internet security, configuration management, domain and DNS management, as well as backup and restore processes.

Continuous monitoring of the network, hardware, and software is carried out 24x7, supplemented by a dedicated help desk available round the clock to address any support issues that may arise.

To swiftly recover from hardware failures, the data centers maintain a pool of spare servers and hardware components.

Additionally, data is backed up on a nightly basis, with offsite storage occurring on a weekly basis to ensure data protection.

PHYSICAL SECURITY	All servers are located in a cat5 data center with 24x7 guard-controlled access. Identification protocols and biometric scanners are used to authenticate technicians before permitting their entry into the data center. Access is strictly limited to personnel that need to work on servers or infrastructure.
TRANSPORT SECURITY	All communication between your PC and your Hosted Remote Desktop environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
FIREWALL SECURITY	All ports into and out of the data center are blocked except for the few ports necessary to provide access to your solution. Intrusion detection provides added security.
WINDOWS SECURITY	DiscoverTec employs the strictest possible Windows lock-down techniques. Users only have access to the functions required for the functioning of their Hosted Remote Desktop solution, and they are securely separated from all other users in the data center. All servers run Windows 2008 R2 or above and any applicable security patches are applied shortly after they become available.
DATA SECURITY	Databases are kept completely isolated, strong passwords are required, and access is strictly limited.
PASSWORD SECURITY	Strong password requirements are maintained for all deployments. These passwords that are made up of combinations of upper and lowercase letters, symbols and numbers are extremely effective in preventing unauthorized access.
VIRUS SECURITY	Microsoft Forefront software is employed and kept continually up to date to ensure a clean, safe environment.

Track record – Gateway²Britain

- The G²B project selected and tested selected track-and-trace technologies, including EyeSeal.
- 38 shipments from Flanders to the UK were simulated and 29 shipments were followed up via T&T technologies.
- The data-sharing platform offered increased automation, and better visibility of data, resulting in time savings, fewer errors, and reduced emails.
- Track & trace technologies provided a better understanding of the location, conditions, and safety of goods.
- Combining the transparent trade lane and data-sharing pillars reinforced transparency in the logistics flow.
- The G²B platform offers benefits for both private and public parties such as customs and FASFC.

EyeSeal was selected as the best internal container monitoring solution during this project

Countries visited in worldwide deployments since 2018

ALBANIA
ARGENTINA
AUSTRALIA
BAHAMAS
BELGIUM
BOLIVIA
BRAZIL
CAMBODIA
CANADA
CHILE
CHINA
COLOMBIA
CROATIA
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
FRANCE
GERMANY
GREECE
GUATEMALA
HONG KONG
INDIA
INDONESIA
IRELAND
ISRAEL
ITALY
KENYA
MALAYSIA
MALDIVES
MAURITIUS
MEXICO
MYANMAR
NICARAGUA
NORWAY
OMAN
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REUNION ISLAND
RWANDA
SAUDI ARABIA
SEYCHELLES
SINGAPORE
SOUTH AFRICA
SPAIN
SRI LANKA
SWITZERLAND
TAIWAN
TANZANIA
THAILAND
THE NETHERLANDS
TRINIDAD & TOBAGO
TURKEY
U.S. VIRGIN ISLANDS
UGANDA
U.A.E.
UNITED KINGDOM
URUGUAY
U.S.A.
VENEZUELA
VIETNAM

The solution for the entire value chain

Shipper
- Brand protection
- Increased efficiency
- Secure supply-chain

Surveyors & freight forwarders
- Streamlining of operations
- Revenue opportunity
- Positive for reputation

Trade finance
- Reduced fraud
- Improved transparency
- Increased revenue

Governments
- Homeland security
- Crime mitigation
- Increased tax revenue

Shipping companies
- Increased safety
- Reduced liability

Cargo terminals
- Higher efficiency
- Reduced congestion
- Increased safety

Law enforcement
- Rule of law
- Efficiency
- Less negative impact on society

Customs
- Higher efficiency
- Secure borders
- Increased data visibility

Insurance
- Improved risk assessment
- Efficient claims processing
- Increased profitability
- Reduced instances of fraud

Digital platforms
- Lack of reliable devices
- Reliable data
- Added value services

Ground transportation
- More control
- Increased safety
- Increased efficiency

Final customer
- No surprises
- No disruptions
- Increased satifcation