World Customs
Organization

Study Report on Smart Security Devices (SSDs)

2025

wcoomd.org

STUDY REPORT ON SMART SECURITY DEVICES (SSDs)

2025

World Customs Organization

CONTENTS

FOREWORD BY THE WCO SECRETARY GENERAL

As the representative of Customs administrations globally, the World Customs Organization (WCO) is committed to assisting Members in their efforts to facilitate legitimate trade. Meeting this commitment requires a focus on efficiency, innovation and collaboration across borders. As international trade volumes continue to rise, Customs administrations must be prepared to clear goods more efficiently without compromising on their commitment to protect society or disrupting international supply chains. In this context, technology plays an essential role in addressing both security and facilitation needs.

The adoption of Smart Security Devices (SSDs) by Customs administrations represents a significant step forward in leveraging digital solutions to enhance the security of global supply chains. These devices offer a comprehensive approach to monitoring and securing cargo, providing real-time data that help prevent illicit activities, such as smuggling and theft, while optimizing Customs procedures.

The WCO has long recognized the importance of innovation to enable Customs procedures to remain responsive to emerging threats and trends. With the growing integration of Internet of Things (IoT) technologies, SSDs are setting a new standard for container security. This study report highlights the benefits, challenges, and opportunities that SSDs present, emphasizing their role in advancing both trade security and efficiency.

Through the collective efforts of Customs administrations, the private sector, and international organizations, we can continue to improve the integration of these technologies into everyday Customs operations. This report is an invaluable resource, providing essential insights into how SSDs can be implemented effectively across diverse global contexts, contributing to a safer and more transparent international trade environment.

I encourage all stakeholders to use this study as a foundation for discussions, collaboration, and innovations that will shape the future of Customs operations in an increasingly digital world.

IAN SAUNDERS

SECRETARY GENERAL, WORLD CUSTOMS ORGANIZATION

INTRODUCTION

SECURING AND FACILITATING THE SUPPLY CHAIN

As the global trade agenda focuses largely on securing and facilitating trade, it requires a robust framework for the Customs-Business dialogue on the growing adoption of technologies to sustain legitimate trade growth. As identified by many studies, efficient trade logistics is a critical link to effective trade facilitation. Changes in supply chain performance are to be implemented in areas including procedures systems and overall interconnectivity. Technology and innovation are key mechanisms through which trade can translate into growth.

Digitalization can enhance competitiveness, and as businesses seek to contain or cut logistics and supply-chain management costs, carriers, shippers, traders, information and communication technologies (ICT) service providers are striving to enhance supply-chain visibility and analytics.

During the last decade, various large-scale initiatives led by key supply chain stakeholders[1] have been launched to enhance situational awareness, enable end-to-end visibility and performance monitoring, and provide decision-support tools. These initiatives combine track and trace devices and interconnected sensors to provide international supply chains with smart systems and operating models with enhanced capabilities to utilize available information to monitor service performance and cargo integrity.

Monitoring and securing cross-border cargo is also a strategic imperative for Customs. Various Customs administrations have already undertaken initiatives with the use of track and trace technologies (including Smart Security Devices, SSDs, to enhance the effectiveness of Customs supervision.

This concomitant use of technologies at different points of the supply chain and by different stakeholders creates opportunities to identify collaboratively the specifics of the technologies used to secure, monitor and track multimodal cargo through its life cycle. This could be done with a view to paving the way for enhanced Customs-Business interoperability through collaborative work on standardization.

[1] Carriers have embraced connected products and technologies for high value cargo over the last few years, with some of the largest shipping companies progressively equipping reefer fleets with the Internet of Things (IoT) technologies, or cooperating in a move towards interoperability and open standards for monitoring containers.

CHAPTER 1

BACKGROUND AND TRENDS: FROM CONTAINER SECURITY DEVICES TO SMART SECURITY DEVICES FOR CONTAINERS

CAIU 221970 22G1
MAX. GROSS 30.480 KGS. 67.200 LBS.
TARE 2.200 KGS. 4.850 LBS.
NET 28.280 KGS. 62.350 LBS.
CU. CAP. 33.2 CU.M. 1.170 CU.FT.
QNLU 100008 22G1
MAX. GROSS 30.480 KGS 67 200 LBS
TARE 2.230 KGS 4.920 LBS
NET 28.250 KGS 62.280 LBS
CU.CAP. 33.2 CU.M. 1.173 CU.FT.
VSBU 20683 22G1
VSBU 200698 22G1
VSBU 201889 22G1
PMLU 20117 22G1
CRXU 342802 22G1
QATAR NAVIGATION
BEACO

1

THE WCO'S TOOLS PROVIDE A CLEAR AND EXPLICIT LEGAL FRAMEWORK ON CONTAINER SECURITY DEVICES (CSDS). ALL CONTAINER ACCESSORIES OR EQUIPMENT COMPRISING THE ABILITY TO DETECT TAMPERING OR INTRUSION CAN BE CONSIDERED AS CSDS.

The Recommendation of the Customs Cooperation Council (CCC) concerning the Customs formalities in connection with the temporary admission of Container Security Devices of June 2013 defines a CSD as:

"an accessory or a piece of equipment that can be affixed to, on, [or] inside, or form part of, a container or a load compartment and which is intended to detect tampering or intrusion into the container or load compartment either through either door or through any other side. CSDs include mechanical and electronic seals. The device may or may not be reusable and may or may not have additional functionalities such as monitoring the status of the goods and container tracking."

This definition, therefore, covers devices such as (without the list being exhaustive):

- Mechanical seals.
- E-seals.
- Track and trace devices with the appropriate sensors detecting tampering or intrusion, and possibly also allowing tracing if the location of the container or the goods.
- Smart container devices offering real-time or near real-time monitoring of the container and cargo integrity.

The Recommendation is primarily aimed at addressing the issue of granting temporary admission to any such devices (be they CSDs, or mechanical or electronic seals). The Recommendation does not distinguish more specifically between CSDs and mechanical or electronic seals.

However, there is a fundamental difference between mechanical seals and the numerous electronic devices which are increasingly being used as part of the digitalization of the international supply chain. The quality and granularity of the available data enable interoperability between previously siloed processes or systems, either through data-rich information collected and processed by electronic devices, or through secured and structured data feed through data pipelines.

The need to capture and aggregate data to better manage trade lanes has resulted in the increased use of connected sensors and tracking devices. Tracking, monitoring and securing containers is part of the development of global systems providing enhanced decision-making tools for the whole supply chain. For example, it can assist Customs to determine the nature of the control or procedure (e.g. NII inspection or physical inspection) that a shipment should be subjected to.

The drive for visibility and transparency throughout the entire supply chain is leading to the growing adoption of Smart Security Devices (SSDs). In addition, SSDs have added features such as status checking, location tracking, protection and encryption, thus allowing real-time communication and exchange of data.

SCOPE

It is essential to define clearly the devices which are the subject of this Study Report in order to develop an inclusive and common understanding in this matter.

As outlined in the CCC's Recommendation, "CSD" provides a wide definition, encompassing mechanical or electronic devices. An appropriate terminology should therefore be adopted to guide the collaborative efforts between Customs and stakeholders in this respect.

It is equally important to define what type of data Customs requires to effectively perform its mission and integrate digital opportunities.

An "e-seal" has been defined in ISO 18185 as a "read-only, non-reusable freight container seal conforming to the high-security seal defined in ISO 17712 and to this international Standard that electronically provides evidence of tampering or intrusion through the container doors".

An ISO 18185-compliant seal also has very limited track and trace capabilities, essentially limited to the reading of locations and times.

"Smart containers" are focusing on ISO-standardized seagoing containers, including reefers, dry or tank containers used for multimodal cargo transport fitted with electronics enabling logistics "door-to-door" tracking and monitoring. It is important to note that not all containers are equally suited to becoming smart containers. The feasibility and cost of retrofitting a container with smart technology will vary depending on the container's size, purpose, and the complexity of the monitoring and communication requirements. Additionally, regulatory and safety considerations may come into play, especially if the container is to be used in specific industries like pharmaceuticals or food storage.

For the purposes of this Study Report, the focus is on enhancing security and facilitation, keeping the scope of application open and independent from a specific mode of transport. The Study Report remains neutral regarding technology and devices, without endorsing any particular vendors or their products.

It is important to acknowledge that technology is developing rapidly, and that providers are building different systems in a highly competitive market; this Study Report does not prescribe any specific technology, rather explores various opportunities for meeting both the performance and compliance needs of Customs and Business by using Smart Security Devices.

It is, therefore, imperative to adopt a clear terminology so as to provide an accurate framework to promote transparent criteria for connected devices used in securing cargo integrity and transport equipment, and in supervising specific Customs procedures linked to securing and facilitating trade, and to foster essential interoperability with business practices.

CHAPTER 2

SMART SECURITY DEVICES FOR ENHANCED LOGISTICS AND SUPPLY CHAIN MANAGEMENT

TARE
NET
CU. CAP.
SURALOC
CUSTOMS
INSPECTOR

Smart Security Devices (SSDs) offer immense potential for enhancing logistics safety, security, and efficiency, as well as enabling track, monitor, and trace capabilities in national and international transits. At the same time the security risks posed by unauthorized access to supply chain data and intentional tampering need to be considered thoroughly and managed. This section delves into the opportunities, benefits, and challenges associated with the widespread implementation of SSDs in Customs, supply chain management, and cargo movements. Furthermore, it outlines the essential considerations and actions necessary to address these challenges and create a robust framework for the seamless integration of SSDs.

2.1 LEVERAGING OPPORTUNITIES FOR ENHANCED SUPPLY CHAIN MANAGEMENT

LOGISTICS SAFETY, SECURITY AND EFFICIENCY

SSDs present an opportunity to bolster the safety and security of cargo against unlawful intrusion, robbery, drug trafficking, and smuggling. By integrating SSDs into the Customs and logistics landscape, there is a possibility to empower economic operators to respond promptly to potential threats, thereby safeguarding cargo and ensuring smooth operations throughout the supply chain.

TRACK, MONITOR AND TRACE CAPABILITIES

The advanced data provided by SSDs on the status and location of means of transport and cargo allows Customs and economic operators to take timely action and prevent illegal behaviour. The ability to trace the journey of goods ensures transparency and builds trust among all stakeholders involved, but only when data security and appropriate access controls are assured.

INTEGRATED SUPPLY CHAIN MANAGEMENT

Seamless data exchange through SSDs and applying analytics to this information enables integrated supply chain management, ensuring the quality and timing of shipments. Improved visibility of data when provided securely can enhance supply chain efficiency and productivity while reducing delays and costs.

2.2 UNVEILING THE BENEFITS OF SMART SECURITY DEVICES

STRENGTHENED SECURITY AND REDUCED RISK

Implementing SSDs can lead to enhanced cargo security, instilling confidence in Customs and economic operators against illicit activities. By curbing incidents of intrusion, tampering, and hacking attempts, the risks associated with cargo movements are significantly minimized. However, as highlighted above, appropriate security and controls on access to the data must be implemented to ensure these benefits.

PROMPT DECISION-MAKING

Some SSDs furnish real-time updates on the status and integrity of cargo, enabling quick decision-making for Customs and economic operators. Timely intervention in response to critical events ensures smoother Customs clearance and improves cargo flow.

IMPROVED SUPPLY CHAIN EFFICIENCY

Through better visibility, SSDs contribute to a more streamlined and efficient supply chain. This efficiency translates into increased productivity, reduced costs, and a competitive advantage in the global market.

2.3 CONFRONTING THE CHALLENGES TO SUCCESSFUL IMPLEMENTATION

ENSURING DATA SECURITY AND AUTHENTICATION

While SSDs offer valuable insights, maintaining data security and ensuring data confidentiality and authenticity remain paramount concerns. Robust cyber security measures must be in place to safeguard against unauthorized access and potential data manipulation. In the context of this Study Report, it is important to note that during testing SSDs can be susceptible to relatively uncomplicated methods, such as the use of Faraday bags to disrupt their signals. Additionally, they can also be compromised through physical means, such as being damaged or removed as a result of a direct attack on the container housing the SSDs. These vulnerabilities underscore the need for robust security measures to protect the integrity and functionality of SSDs in various operational scenarios.

ADDRESSING DATA QUALITY AND OWNERSHIP

Addressing data quality and ownership when applying SSDs is essential to ensure the integrity and accuracy of data associated with cargo shipments. The example below illustrates how this could be achieved:

- Clearly defining data ownership within the customs process. It is crucial to determine who is responsible for managing and maintaining data related to SSDs. This could involve collaboration between customs authorities, shipping companies, and other stakeholders.
- Developing a robust data governance framework specific to customs operations. This framework could outline the roles, responsibilities, and processes for managing data quality and ownership. Ensuring that all parties involved understand their obligations is equally important.
- Defining data quality standards that are specific to the use of SSDs. These standards could cover data accuracy, completeness, consistency, and timeliness, particularly in the context of customs declarations and cargo tracking.
- Implementing data validation mechanisms within the e-seal and SSD systems. Data transmitted by these devices should ideally be validated for accuracy and authenticity. Unauthorized access or tampering should trigger alerts or notifications.
- Prioritizing data security to prevent unauthorized access and data breaches.
- Implementing robust auditing and logging mechanisms to track data access and changes.
- Training customs personnel, shipping companies, and other stakeholders on data quality and ownership responsibilities.
- Complying with relevant data privacy regulations and customs standards.

MITIGATING COSTS AND ESTABLISHING RESPONSIBILITY

Given the diverse range of devices, business models, and operating procedures, determining the costs and responsibility for SSD implementation can be complex. Practical case studies, exploring various working models, could offer valuable insights for stakeholders.

OVERCOMING LOGISTICAL AND ICT INFRASTRUCTURE CHALLENGES

Temporary admission and return logistics of SSDs require streamlined procedures and efficient ICT infrastructure.

The implementation of SSDs offers a promising solution for revolutionizing logistics safety, supply chain management, and Customs operations. By embracing the opportunities, understanding the benefits, and confronting the challenges, Customs administrations and economic operators can forge a secure and efficient future for international trade. A collaborative effort among stakeholders, backed by robust regulations and standards, could pave the way for the widespread adoption of SSDs, ensuring a safer and smarter global supply chain ecosystem.

CHAPTER 3

STANDARDS FOR SSDs

3

3.1 EXISTING STANDARDS

ISO STANDARDS

ISO 10374:1991 is a standard for Radio Frequency Identification (RFID) automatic identification of freight containers. It specifies all necessary user requirements: a container identification system, data coding systems, description of data, performance criteria and security features. It is associated with ISO/TS 10891:2009, which is an updated version, but ISO 10374:1991 has not been removed as the standard is still in use in some countries.

ISO/TS 10891:2009 Freight containers - Radio frequency identification (RFID) - Licence plate tag.

ISO/DTS 7344 Short-range Wireless Sensor to Device Communication.

ISO/IEC 15417:2007 specifies the requirements for the bar code symbology known as Code 128. It specifies Code 128 symbology characteristics, data character encoding, dimensions, decoding algorithms, and the parameters to be defined by applications. It specifies the symbology identifier prefix strings for Code 128 symbols.

ISO 17363:2013 Supply chain applications of RFID - Freight containers.

ISO 17712:2013 establishes uniform procedures for the classification, acceptance, and withdrawal of mechanical freight container seals. It provides a single source of information on mechanical seals which are acceptable for securing freight containers in international commerce.

ISO 18000-6 is an international standard governing the way tags and readers communicate in the UHF spectrum. There are currently three versions: 18000-6A, 18000-6B and 18000-6C. Of these, 18000-6C is by far the most commonly used.

ISO 18185 is an international standard that provides an unambiguous and unique identification of the container seal, its status and related information. The presentation of this information is provided through a radio communications interface providing seal identification and a method for determining whether a freight container's seal has been opened. It includes active protocols, enabling both simple low cost and more robust seals. ISO 18185 consists of the following parts, under the general title Freight containers - Electronic seals:

- Part 1: Communication protocol.
- Part 2: Application requirements.
- Part 3: Environmental characteristics.
- Part 4: Data protection.
- Part 5: Physical layer.

ISO 18186:2011 Freight containers - RFID cargo shipment tag system.

ISO/TS 18625:2017 Freight containers - Container Tracking and Monitoring Systems (CTMS): Requirements.

ISO/AWI 23354 Business requirements for end-to-end visibility of logistics flow (under development).

ISO 23359 is a new body of work for read/write RFID for freight containers.

ISO/TS 24533:2012 Intelligent transport systems - Electronic information exchange to facilitate the movement of freight and its intermodal transfer - Road transport information exchange methodology.

ISO 9001:2015 specifies requirements for a quality management system when an organization:

a. needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and

b. aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

UN/CEFACT STANDARDS

UN/CEFACT Transport and Logistics has established a Smart Container Project.

This Project is working on use cases which could be used to identify some elements on the required data set for SSDs such as:

- ETA Update.
- Actual Executed Transit Time.
- Trip Tracking.
- Haulage Container Time and All Routing Points Passed.
- Exception Alerts.
    - Schedule Deviation Alert.
    - Unexpected Door Opening.
    - Unexpected Temperature or Humidity Change.
    - Overlanded Container.
- Fast Lane for Cross-Border Agency.

3.2 CYBER SECURITY STANDARDS

The cyber security standards to be considered are tied to the cyber security and supply chain cyber security standards. The use of SSDs and the increasing reliance of governments and business on these ICT products and services results in potential threats to supply chains, including the threat of intentional tampering during operations. Standards need to be identified to ensure that the SSDs used for Customs processes are reliable, report any hacking attempts, are not infiltrated, and are free from substitution with counterfeit components, etc.

Cyber security should be part of the device requirements so that any device sold is, by design, cyber safe. Development and recognition of cyber security standards are key for Customs to integrate the smart security devices for containers into the trust chain efficiently.

3.3 GAPS AND FUTURE CONSIDERATIONS

Given the rapid evolution of the industry and the ongoing discussions about standardization of technologies to ensure interoperability, it is essential to have close and proactive monitoring of the different measures and steps impacting directly or indirectly the SSDs for container production and usage.

One of the areas for future consideration could be the issue of the compatibility of SSDs. Compatibility, in the context of SSDs, refers to the ability of these devices to seamlessly integrate with existing Customs and border management systems, as well as with other stakeholders in the supply chain. Achieving compatibility is critical for several reasons:

a. Interoperability: compatibility ensures that SSDs can work harmoniously with various technologies and systems utilized by customs administrations and trade partners. This promotes the efficient exchange of data and information.

b. Avoiding disruption: incompatible SSDs can disrupt the flow of goods, delay inspections, and increase costs for both customs authorities and traders. Compatibility is essential to prevent such disruptions.

c. Consistency: compatible SSDs help maintain consistency in security protocols and procedures across borders, reducing vulnerabilities and potential gaps in security.

While compatibility is essential, several challenges must be taken into consideration:

a. Customs administrations and trade partners employ diverse technologies and systems. Achieving compatibility in this heterogeneous landscape can be complex.

COMPATIBILITY IS AN IMPORTANT ASPECT OF SSDs IN THE CONTEXT OF MODERN TRADE.

b. Inconsistent data standards can hinder data sharing and interoperability.

c. Upgrading existing systems and integrating SSDs can be costly. Customs administrations and stakeholders must carefully allocate resources.

d. Ensuring compatibility should not compromise security. Striking a balance between interoperability and safeguarding sensitive information is paramount.

Navigating the intricacies of compatibility remains a challenging endeavour, and it is important to note that no clear-cut solutions have emerged so far. However, it is evident that further research and collaborative efforts are imperative in this domain. In the absence of definitive answers, some general categories of potential solutions to explore include:

a. Developing international standards for data formats, communication protocols and encryption methods to facilitate compatibility.

b. Collaboration between customs administrations, international organizations, and private sector stakeholders to define common goals and share best practices.

c. Training customs officials and stakeholders on SSD deployment and maintenance to enhance compatibility.

d. Establishing clear regulatory frameworks that encourage the use of compatible SSDs and provide guidelines for their deployment.

Compatibility is an important aspect of SSDs in the context of modern trade. There is a clear need for continuing research and cooperation among stakeholders to overcome compatibility challenges and maximize the benefits that SSDs could offer to the global trade community.

CHAPTER 4

TYPES AND FEATURES OF SMART SECURITY DEVICES

Hapag-L
32 500 kg
71 650 lbs
3 950 kg
8 710 lbs
EPAIR WITH
"CORTEN"
EL ONLY
SAMSUNG

4

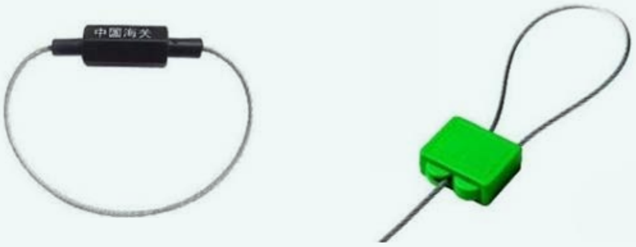
According to different application features and functions, SSDs can be classified into passive or active SSDs and semi-active SSDs.

4.1 PASSIVE DEVICES

Passive SSDs are a category of security technology used in the context of supply chain and border security. Unlike active SSDs, which actively transmit or generate signals or data, passive SSDs do not emit any signals or require a power source to operate. Instead, they rely on their physical or chemical properties to provide security-related information.

FORME PRINCIPALE

Dispositifs de verrouillage passifs



MAIN FUNCTION

Passive SSDs incorporate a data recording identification chip, which allows data to be written only once, preventing further alterations. This chip is seamlessly integrated with the mechanical seal, making it tamper-proof, as it cannot be extracted without causing destruction.

To identify and read the data, a matched chip data reader is essential for passive SSDs. An incorrect data reading or identification may indicate intentional tampering, leading to manual inspection and necessary countermeasures.

The passive SSD utilizes RFID technology to power the data reading circuit. The device receives energy from the reader through its antenna via electromagnetic waves. The communication range typically extends up to 2 metres, ensuring reliable and secure data transfer. it is characterized by affordability, high quality, compact dimensions, and complete independence from external power sources. However, no real-time readings/ communications are possible.

Some key characteristics and examples of passive SSDs include:

No power source: passive SSDs do not have built-in power sources like batteries or electronic components. They do not actively transmit signals or generate data, making them less conspicuous and immune to electronic detection.

Indirect information: these devices provide security-related information indirectly through changes in their physical properties or reactions to external stimuli. For example, a passive SSD might change colour, shape, or magnetic properties when exposed to specific conditions or triggers.

Covert deployment: passive SSDs can be covertly integrated into packaging, labels, or items in the supply chain. This makes them suitable for covert tracking and authentication purposes.

Examples: common examples of passive SSDs include tamper-evident seals, security inks, and RFID (Radio-Frequency Identification) tags that only become active when exposed to specific radio frequencies from a reader.

Tamper detection: some passive SSDs are designed to detect tampering or unauthorized access. When someone tries to open a package or container protected by a passive SSD, it may break or change in a way that is easily detectable.

Authentication: passive SSDs can also be used for product authentication. For instance, a passive SSD label on a high-value item can be checked for authenticity by verifying its unique physical characteristics when exposed to specific conditions.

Passive SSDs are particularly useful in situations where discreet monitoring or authentication is required without revealing the presence of security measures to potential threats. Their reliability and effectiveness depend on the specific design and technology employed, making them a versatile option in the realm of supply chain security and anti-counterfeiting measures.

4.2 SEMI-ACTIVE DEVICES

Building upon the passive SSD, the semi-active variant incorporates data storage and an RFID electronic circuit. Additionally, a small battery powers the internal circuits to operate efficiently. This configuration offers a notable advantage: the antenna can focus solely on data transmission, without the need to receive electromagnetic wave energy from the reader. Compared to passive devices, semi-active devices exhibit faster response times and enhanced efficiency. Each semi-active device is equipped with an exclusive RFID chip number, further contributing to its uniqueness and reliability.

MAIN FORM

A semi-active device is an upgraded version of the passive SSD, offering improved functionalities. Unlike passive devices, semi-active devices enhance information transmission efficiency and information storage capacity. However, it is important to note that semi-active devices do not feature the same 2G/3G/4G network communication capabilities as active devices.

MAIN FUNCTION

Semi-active devices incorporate a data recording identification chip that allows data to be written only once, preventing further modifications. This chip is securely integrated with the mechanical seal, making it non-removable, and will be rendered unusable if tampered with.

To identify and read the data, a matched chip data reader is required for semi-active devices. Unsuccessful data reading or identification indicates potential tampering, leading to manual intervention and necessary precautions.

Semi-active devices utilize RFID technology, and the built-in battery powers the data reading circuit. With a communication range of 5-10 metres, semi-active devices surpass the reach of passive devices. Moreover, semi-active devices are characterized by their cost-effectiveness, superior quality, and compact size.

Some key characteristics and features of semi-active SSDs include:

Limited activity: semi-active SSDs are not continuously active like fully active devices that transmit data regularly. Instead, they are more selective in their activity, only becoming active in response to specific triggers or conditions.

Power source: unlike passive SSDs that do not require a power source, semi-active SSDs typically have a limited power source, such as a small battery. This power source allows them to perform certain actions or transmit data intermittently.

Event-driven: these devices are event-driven, meaning they activate in response to predefined events or stimuli. For example, a semi-active SSD attached to a cargo container might activate when the container is opened or when specific environmental conditions are met.

Versatility: semi-active SSDs can be designed for various purposes, including tamper detection, environmental monitoring, or tracking. For instance, they may include sensors to detect temperature, humidity, or shock, and transmit data if these conditions exceed preset thresholds.

Covert operation: similar to passive SSDs, semi-active devices can be covertly deployed within the supply chain, making them suitable for security and anti-counterfeiting applications where discreet monitoring is essential.

Extended lifespan: while semi-active SSDs have a limited power source, they are often designed to have a longer lifespan compared to fully active SSDs, as they only activate in specific situations

Examples of semi-active SSDs include security seals that use a battery to send an alert when tampering is detected, or RFID tags with environmental sensors that transmit data when specific conditions are met.

4.3 ACTIVE DEVICES

Active SSDs are advanced security technologies used in supply chain and border security, known for their ability to actively transmit data and communicate with monitoring systems. These devices are equipped with power sources, sensors, and communication capabilities to provide real-time or scheduled information about the status and security of items, containers, or assets.

MAIN FORM

Active devices come in various types based on their installation position, including the hanging hole type, lifting pole type, magnetic type, and more. It is important to note that other installation methods are also possible, and the list provided serves only as an illustration.

Hanging hole type devices can be installed in the container's lock hole. Containers manufactured after ISO 14961/Amendment 5 became effective typically have an alternative sealing location known as the "SecuraCam," regardless of whether they have seal eyes on the container door handles. Lifting pole type devices are meant to be installed between the second and third lock rods of the container. On the other hand, magnetic type devices are designed to be installed through magnetic absorption at various positions, including the corners of the container.

ACTIVE DEVICES

MAIN FUNCTIONS

Compared with traditional mechanical seals and passive devices, active devices have many extended functions.

The table below shows some examples of these:

SN	FUNCTIONS	PASSIVE DEVICE	SEMI-ACTIVE DEVICE	ACTIVE DEVICE
1	Seal and unseal	●	●	●
2	Data collection/storage	●	●	●
3	Satellite positioning	–	–	●
4	Cellular data communication	–	–	●
5	Data encryption	–	–	●
6	Alarm detecting	–	–	●
7	Remote control	–	–	●
8	Wireless upgrading	–	–	●
9	Data interface	–	–	●

Some key characteristics and features of active SSDs include:

Continuous activity: active SSDs are continuously active and transmit data at regular intervals or on demand. They maintain an active connection with monitoring systems or networks, allowing for real-time tracking and monitoring.

Power sources: active SSDs are powered by built-in power sources, such as batteries or rechargeable cells. This continuous power supply enables them to operate for extended periods without relying on external power.

Data transmission: these devices can transmit a wide range of data, including location, temperature, humidity, shock or impact, and security status. The data is sent to centralized monitoring systems or can be accessed remotely via secure networks.

Real-time tracking: active SSDs are well-suited for real-time tracking and monitoring of cargo, assets, or inventory.

Security features: active SSDs often include security features such as tamper detection and intrusion alerts. If unauthorized access or tampering is detected, the device can trigger an immediate alert.

Two-way communication: many active SSDs are equipped with two-way communication capabilities. This allows for remote configuration, updates, and interaction with the device, enhancing control and security.

Customizable parameters: users can often customize parameters and settings for active SSDs, allowing them to tailor the device's functionality to specific security and monitoring requirements.

Integration: active SSDs are designed for integration with existing monitoring and logistics systems, making it easier for organizations to incorporate them into their operations.

Examples of active SSDs include GPS trackers, temperature and humidity monitoring devices, and security sensors. These devices are widely used in logistics, transportation, and supply chain management to enhance security, improve visibility, and ensure the integrity of goods and assets throughout their journey.

Active SSDs offer real-time tracking and monitoring advantages but come with weaknesses compared to passive and semi-active SSDs, including their power dependency, higher cost, maintenance requirements, increased visibility to potential threats, technical complexity, potential environmental impact from battery disposal, data overload risks, limited covert capabilities, and relatively shorter battery life.

COMMUNICATION FREQUENCY

The RFID communication frequency should comply with related international/national/regional laws and regulations for communication. International public frequency can be used. At present, a variety of international public frequencies are available, among which 433 MHz and 2.45 GHz are the most frequently used.

Parameters of 433 MHZ physical layer

PARAMETER	DESCRIPTION
Centre frequency (default transmission frequency)	434.4 MHz
Transmission rate	50 kbps
Receiving sensitivity	-90 dBm @ 50 kbps
Modulation system	GFSK
Maximum frequency error	±58 kHz
Maximum receipt signal	0 dBm
Transmitting power	(1) Programmable (maximum): +10 dBM (2) In compliance with local requirements

Parameters of 2.45 GHz physical layer

PARAMETER	DESCRIPTION
Range of communication frequency	2,400— 2,483.50 MHz
Centre frequency (default transmission frequency)	2441.750 MHz
Occupied bandwidth	60 MHz
Transmitting power	(1) Programmable (maximum): +10 dBM (2) In compliance with local requirements

PARAMETER	DESCRIPTION
Default transmission rate	9.6 kbps
Receiving sensitivity	-90 dBm @ 10 kbps
Modulation system	FSK
CRC polynomial	CCITT polynomial G (X) = (X16 + X12 + X5+1)
CRC polynomial initial value	0xFFFF

COMMUNICATION DISTANCE

The interference-free communication distance between active device and handheld reader should be based on the actual use case scenario. For application in the bayonet system, the interference-free communication distance with the reader fixed on the bayonet is based on the use case requirement. When the smart security lock is installed on the container door, its sealing, unsealing, satellite positioning, networking, alarming and electric quantity status is displayed through the indicator light.

COMMUNICATION PROTOCOL

The communication protocol should comply with the air interface protocol of related frequency bands specified in ISO/IEC18000.

1. Information technology – Radio frequency identification for item management – Part 1: reference architecture and definition of parameters to be standardized (ISO/IEC 18000-1).
2. Information technology – Radio frequency identification for item management - part 2: parameters for air interface communications below 135 kHz (ISO/IEC 18000-2).
3. Information technology – Radio frequency identification for item management – part 3: parameters for air interface communications at 13,56 MHz (ISO/IEC 18000-3).
4. Information technology – Radio frequency identification for item management – part 4: parameters for air interface communications at 2,45 GHz (ISO/IEC 18000-4).
5. Information technology – Radio frequency identification for item management – part 6: parameters for air interface communications at 860 MHz to 960 MHz (ISO/IEC 18000-6).
6. Information technology – Radio frequency identification for item management – part 7: parameters for active air interface communications at 433 MHz (ISO/IEC 18000-7).

DATA ENCRYPTION

Encryption is necessary for data storage and transmission in active devices. The encryption algorithm should comply with relevant national/regional regulations, recognizing that containers move across-borders internationally.

The encryption algorithm supports international algorithms, for example RC or RSA or asymmetric cryptographic algorithms or Elliptic-curve cryptography (ECC). Some examples of cryptographic algorithms can be found at https://www.nist.gov/topics/cryptography

BATTERY SUPPLY REQUIREMENTS

Active devices come with an integrated battery, with a battery life that meets the demands of practical applications. If the power consumption exceeds the limit, the internal chip data will promptly be stored to ensure data integrity and avoid any damage or loss.

USER INTERFACE

LED indicator lights, LCDs or buzzer reminders and other user interactive interfaces are designed for active devices to provide operational and alarm reminders and improve operating usability and visual effects.

FEATURES OF THE APPLICATION ENVIRONMENT

To meet the application demands of poor outdoor transportation, active devices need to adapt to all kinds of application environment, including high and low temperature, high humidity, mechanical vibration, salt mist, falling impact, rain/snow sandstorm and electromagnetic interference. According to different national and environmental conditions, the requirements of active devices are also different. Under normal conditions, relevant provisions in IEC60068 and ISO 8185-3 could be taken as the test standard.

1) Low temperature

Active devices should be capable of working normally for the required number of hours under the lowest temperatures of the operating environments, and restoring to normal temperature data and maintaining their integrity after being exposed to the lowest temperature for several hours. The test should comply with the method specified in IEC60068-2-1.

2) High temperature

Active devices should be capable of working normally for the required number of hours under the highest temperatures of the operating environments, and restoring to normal temperature data and maintaining their integrity after being exposed to the highest temperature for several hours. The test should comply with the method specified in IEC60068-2-2.

3) Impact

Active devices should be able to withstand impact from the three axial directions for three times respectively under the testing environment of half-cycle sine wave. The device shall operate normally during and after the test. The test should comply with the method specified in IEC60068 2-6.

4) Vibration

Active devices should be capable of working normally under the required testing environment, for example scanning range, scanning speed: 1 oct/min, scanning time: 30 minutes in each direction, peak value at the amplitude of 5-11 Hz: 10 mm and 50 m/s^2 under the acceleration of 11-300 Hz, direction of vibration: three axes.

5) Humidity

Active devices should operate as normal for a period of several hours (e.g. 48 hours) under the testing environment, for example +40° and 95% non-condensing humidity. The test should comply with the method specified in IEC60068-2-78.

6) Shell protection

The shell IP code must comply with the IP55 high-class waterproof and dustproof requirements. The test should comply with the method specified in IEC 60529.

7) Salt mist

No corrosion should be present following storage for a period of several hours (e.g. 48 hours) in the required testing environment, for example 5% NaCl solution, settlement: 1-2 ml/80 cm^2/h, temperature: 35°. The test should comply with the method specified in IEC60068-2-11.

8) Fall

In the three directions (X/Y/Z), the devices must be free from damage when they fall from the specified height, for example 3.5 m onto cement and steel surfaces. After the test, the devices should operate as normal. The test should comply with the method specified in IEC 60068-2-31 and IEC60068-2-32.

9) Electromagnetic compatibility

The radiated susceptibility should comply with relevant requirements in IEC61000-4 (field intensity: 24 V/m, frequency band: 20-1000 MHz, judgment grade: Class B).

The electrostatic discharge should comply with the relevant requirements in ISO 10605, and devices should be capable of withstanding the test under, for example 7 KV contact discharge and 14 KV air discharge (judgment grade: Class B).

APPLICATION FIELDS

Active devices could be used for a host of activities, such as real-time status supervision, data security encryption and multi-cyclic utilization, bonded area supervision, and cross-border logistics supervision, etc.

CHAPTER 5

FUNCTIONALITY OF SOME THE SSDs IN CUSTOMS CLEARANCE

5

DEVICE	OVERVIEW	FUNCTIONALITY	IMPACT ON AUTOMATION
Electronic security devices with GPS	Global Positioning System (GPS) devices are integral to modern logistics and supply chain management, especially in the context of international trade	These devices are attached to cargo containers and vehicles to provide real-time location tracking. The GPS coordinates are continuously sent to a centralized Customs database. This enables Customs officers to automatically validate the cargo's route against the declared information	The use of GPS devices allows for a seamless transition from manual tracking methods to automated systems, capable of handling large volumes of cargo with minimal human intervention
RFID antennas and RFID security devices	Radio-Frequency Identification (RFID) technology is widely used for tracking and identification purposes	RFID antennas and security devices read the RFID tags attached to cargo containers. Once read, this information is wirelessly transmitted to the Customs office's computer system for automatic validation	RFID technology is a cornerstone in the automation of Customs procedures, enabling real-time data exchange and validation, which is crucial for high-throughput environments like ports and border crossings
Licence plate readers	Licence plate readers are specialized cameras equipped with Optical Character Recognition (OCR) technology	These devices are strategically placed at entry and exit points to automatically capture and recognize vehicle licence plates. The acquired data is then sent to the Customs office's computer system for automatic cross-referencing and validation against the declared cargo information	Licence plate readers contribute to the automation of vehicle identification and validation processes, reducing manual errors and speeding up vehicular movement through Customs checkpoints
Container readers	Container readers are advanced scanning devices designed to read and interpret container-specific information	These devices scan barcodes or other identifiers on cargo containers to extract essential information such as container number, weight, and contents	Container readers play a pivotal role in automating the data collection and validation steps in Customs procedures, thereby reducing human error and improving overall efficiency
QR reader for outdoor use	Quick Response (QR) codes are two-dimensional barcodes that can store a variety of data types	Outdoor QR readers are robust devices capable of scanning QR codes in various environmental condition.	The use of QR readers in outdoor settings adds another layer of automation to the Customs clearance process, particularly beneficial in harsh weather conditions where manual operations are challenging

Fml Oil Company
4 Arden Road
Newlands, Harare
Zimbabwe
NVM 6 000 KG
GVM 42 000 KG
ZIMRA

CHAPTER 6

EXPLORING THE VIABILITY OF SMART CONTAINERS AS CUSTOMS SEAL ALTERNATIVES

Over the years, there have been a number of developments in container security devices used by Customs worldwide, ranging from mechanical seals through to e-seals and, mostly recently, IoT-equipped seals. Many of these developments were *incremental* innovations – i.e. a gradual, continuous improvements of existing products.

To effectively address the challenges posed by the increasing volume of international trade transported by containers, it is becoming necessary to explore disruptive innovations, which are characterized by being distinct from traditional and existing solutions. Such innovations hold the potential to make significant improvements in Customs' processes and cope with the evolving demands of the global trade landscape.

The aptly named 'smart container', qualifies as a disruptive innovation which can be used as an alternative to Customs seals and reshape Customs operations.

One of its key advantages is the integration of the features of the previous technological generations with the new ones. Like some types of seals, it can identify unauthorized door openings and, in addition, is capable of providing a context to these events. Geolocation, time stamping and indirect confirmations through additional sensors provide a new, holistic and unrivalled approach to risk management, inspection and Customs operations.

SMART CONTAINERS

Smart containers are ISO shipping containers used in freight and logistics that are equipped with IoT technologies and a range of sensors and devices that deliver:

- Door opening detection.
- Precise gps position.
- Temperature.
- Pressure.
- Humidity.
- Luminosity.
- Impact and container orientation.
- Voc gas.
- And more.

The data collected through the smart container's sensors is transmitted to a central supervision platform, the smart container's 'control tower'. The control tower uses additional information sources, such as Automatic Identification Systems (AIS) and information from shipping companies, to provide a holistic perspective.

There are two main types of smart containers:

1. Regular containers with affixed IoT: regular containers to which an IoT device is affixed permanently or for a certain period of time.
2. Containers with embedded IoT systems: containers in which the IoT hardware was embedded into the original container design during the container manufacturing process.

EMBEDDED IoT	AFFIXED IoT
Always correlated to the same container number	- Can be switched between containers. - Needs administrative and operational efforts to pair a device to its container both physically and in its control tower
The container is "always smart", no more logistics needed after its construction	Logistic efforts are required to install the IoT systems (devices and sensors) to a container and dismount them to use them on another container or to replace them in the event of damage or at the end of any contractual relations between the IoT service provider and the container owner/operators; these could be similar to those required for the existing Customs seals
No risk of IoT device loss	Risk of IoT device loss
Maintenance and repair: the container is not 'smart' if the system is damaged. Maintenance and repair might take time, depending on the damage	Maintenance and Repair: the IoT units can be swapped or an IoT service provider can be replaced by a competitive option
Reports on abnormalities help to detect theft through location updates	Reports on abnormalities help to detect theft through location updates until intentionally broken or removed

The key features and components of smart containers are as follows:

Sensor technology: smart containers are equipped with a range of sensors to monitor conditions such as temperature, humidity, pressure, shock, and location. These sensors provide real-time data on the container's environment and status.

Communication systems: smart containers incorporate communication systems such as GPS, cellular, satellite, or radio-frequency identification (RFID) to transmit data to central monitoring systems. This enables tracking and remote monitoring of the container's location and condition.

Data processing and analytics: smart containers have onboard data processing capabilities, allowing them to analyse sensor data locally or transmit it to cloud-based platforms for more in-depth analysis. This data-driven approach can help optimize logistics operations and detect issues in real-time.

Security features: some smart containers are equipped with security features like tamper-evident seals, intrusion detection systems, and electronic locks.

Temperature control: smart containers used for transporting temperature-sensitive goods, such as pharmaceuticals or perishable foods, often include temperature control systems. These systems can maintain a specific temperature range throughout the journey.

Tracking and monitoring: some smart containers can enable real-time tracking and monitoring of cargo, providing stakeholders with visibility into the container's location, route, and environmental conditions. This information helps optimize supply chain operations and enhance security.

Remote control: in some cases, smart containers offer remote control capabilities, allowing operators to adjust settings or access cargo remotely. This can be particularly useful for troubleshooting or adjusting environmental conditions during transit.

Documentation and compliance: smart containers may facilitate electronic documentation and compliance management by digitally recording and transmitting relevant information, reducing paperwork and streamlining Customs processes.

Integration with IoT: smart containers are often part of the broader Internet of Things (IoT) ecosystem, allowing seamless integration with other IoT devices and systems, such as warehouse management systems and fleet tracking solutions.

Data sharing: data generated by smart containers can be shared with various stakeholders, including shippers, carriers, Customs authorities, and customers.

Smart containers represent a significant advance in the logistics and shipping industries, providing valuable insights, improving cargo safety, and optimizing supply chain processes. They are particularly beneficial for industries with stringent quality and security requirements, such as pharmaceuticals, food, and high-value goods.

At the same time, smart containers are relatively bulky and costly, impacting their scalability and widespread adoption. Additionally, they may not be as versatile as SSDs, as their primary function is cargo transport, limiting their applicability in security-focused or covert monitoring scenarios. Furthermore, smart containers' reliance on power sources, complex maintenance requirements, and potential vulnerability to physical tampering poses challenges in certain deployment contexts.

REGULATORY ASPECTS

Various regulatory organizations are defining the use cases for smart containers, leaving the precise definition out of the scope in order to enable continuous technological developments.

The main requirement for IoT technology is compliance with safety regulations and alignment with the operational needs of the transportation chain.

The challenge for such technology is for it to meet the requirements of international intermodal transportation.

One of the "Operational and Security Awareness" use cases described in the UN/CEFACT Business Requirements Specification (BRS) for Smart Containers relates to "Unexpected Door Opening".

Next steps

As described above, using smart container technology as part of the Customs operation could improve the time efficiency of the processes and improve risk management.

It also encourages cooperation, transparency, and paperless data exchange between stakeholders in the supply chain and reduces logistic efforts.

To further explore the smart container as an alternative to Customs seals and to redefine Customs operations with smart containers, Customs and smart container developers need to continue implementing PoCs (proofs of concept).

Among other things, such PoCs could potentially explore:

1. The data elements to be transmitted from the smart container to the Customs administration.
2. The method by which the data will be transmitted from the smart container to the Customs administration.
3. The intervals at which the data will be transmitted from the smart container to the Customs administration.

307
7.21

CHAPTER 7

OPERATIONAL PROCESSES: DIFFERENT TYPES OF SSDs

7
CUSTOMS
PRODUCT OF COSTA RICA
Dominique

7.1 OPERATING MODE

Different devices operate in various modes due to their specific technical and functional features.

Passive devices do not require a power supply; they draw power from the radio-frequency signals emitted by the reader. These devices offer advantages such as small size, cost-effectiveness, batch reading capability, and long service life. However, they also have limitations, such as a short read distance, limited information storage capacity, and a single operating mode. Passive devices mainly operate through fixed point readers and lack real-time status reporting, making visual real-time supervision challenging. Consequently, they may not be ideal for risk management based on big data, cross-border supervision information sharing, mutual recognition, and low-risk quick release.

Semi-active devices, based on passive devices, include the addition of data storage and RFID electronic circuits but lack real-time communication capability. They are powered by a small

	PASSIVE DEVICES	SEMI-ACTIVE DEVICES
HANDLING	Single operating mode, can only be operated through he reader at the fixed point	Single operating mode, can only be operated through he reader at the fixed point
STORING	Diverse inventory management, master the inventory management by checking the real materials	Diverse inventory management, master the inventory management by checking the real materials
CHARGING	–	A small battery is provided, which is mainly used to drive electronic tag IC, with low power consumption; it does not usually need charging
SEALING	–	After manual sealing, it cannot be unsealed before arriving at the destination
DATA MANAGEMENT AND TRANSFER	Limited storage space, incapable of storing the multi dimensional information to be supervised; the information necessary for management and exchange is confined to the device itself and there is little information about the supervised object, including device ID management, data writing, data reading and data verification	Limited storage space, incapable of storing the multi dimensional information to be supervised; the information necessary for management and exchange is confined to the device itself and there is little information about the supervised object, including device ID management, data writing, data reading and data verification

battery, which enables faster reaction speeds and improved efficiency while maintaining the same operating mode as passive devices.

Active devices, on the other hand, are equipped with GPS, mobile communication, active RFID, and other modules. These devices offer numerous advantages, including substantial information storage capacity, remote real-time operation, and visual supervision. The combination of the supervision platform and active device enables the storage of multi-dimensional information, such as vehicle, cargo, transport, declaration, and place of departure verification details. Throughout transportation, information can be transferred through the supervision platform and device, facilitating mutual recognition of supervision, information sharing, and multi-dimensional vehicle supervision in cross-border Customs transit. Furthermore, when combined with vehicle violation data, active devices enable the application of risk management based on big data.

Specific operating modes of the three types of devices are shown in table form on the following pages:

ACTIVE DEVICES	SMART CONTAINERS WITH EMBEDDED IOT
Diversified operating modes, capable of short-distance operation through the reader or remote operation through he SSD's back end information system	Diversified operating modes, capable of short distance operation through the reader or remote operation through the smart container's control tower
Unified management through the supervision platform, devices will be dispatched in the whole supervision station according to the flow of the supervised vehicles	Not needed in smart containers with embedded IoT
GPS and mobile communication module, built in rechargeable battery	Long life built in rechargeable battery which can be recharged by solar panels
Sealing by handheld devices or remote sealing	Sealing by handheld devices or remote sealing
The supervision platform and device can store supervision related multi dimensional information, including vehicle information, driver information, consigner and cargo information, waybill and Customs inspection image. Data storage is favourable for big data analysis and application based on data supervision (such as risk management, illegal route identification, illegal vehicle identification and illegal cargo identification) and for corresponding processing based on the risk identification situation. For low risk vehicles, it is favourable for improving the Customs transit and border crossing efficiency and realizing quick release	In addition to the "active devices" features, the data is always correlated to the same container number because it is an embedded device which cannot be transferred between containers

	PASSIVE DEVICES	SEMI-ACTIVE DEVICES
MONITORING	Incapable of reporting the position and status information in real time and realizing visual and real time supervision, and only capable of verifying whether the device is abnormal at the checkpoint, en route or at the destination; as no more information about the supervised object can be provided (e.g. cargo, vehicle and departure inspection information), it is limited for verifying and inspecting the cargo information in the transportation process. It may not be very useful for cross border data exchange, mutual recognition of supervision and information sharing	Incapable of reporting the position and status information in real time and realizing visual and real time supervision, and only capable of verifying whether the device is abnormal at the checkpoint, en route or at the destination; as no more information about the supervised object can be provided (e.g. cargo, vehicle and departure inspection information), it is limited for verifying and inspecting the cargo information in the transportation process. It is useful for cross border transportation, mutual recognition of supervision and information sharing
ALARM MANAGEMENT	The destination or the stations along the route can verify the device integrity through the reader	The destination or the stations along the route can verify the device integrity through the reader
RECEIVING	It is unnecessary to recover one off devices, which are to be destroyed after being collected at the destination station. Devices can be recovered for continuous use	It is unnecessary to recover one off devices, which are to be destroyed after being collected at the destination station. Devices can be recovered for continuous use
RETURN LOGISTICS	–	–

ACTIVE DEVICES	SMART CONTAINERS WITH EMBEDDED IOT
Equipped with GPS and mobile communication module, capable of reporting the position and environment status information in real time and realizing real time vehicle supervision through Geographical Information System (GIS) mapping in combination with the logistics supervision platform; the law enforcer can track and check the illegal conveyances	In addition to the "active devices" features, the data is always correlated to the same container number because it is an embedded device which cannot be transferred between containers
In the transportation process, in combination with the position and status information reported by the device, various types of alarm, such as route deviation, illegal stay, overtime stay, illegal opening, journey timeout and abnormal oil volume (oil tank truck), can be defined. The Customs officer can deal with the alarms by different means on the basis of various type of alarm, including field check and dispatching and deployment at the destination	In addition to the "active devices" features, the data is always correlated to the same container number because it is an embedded device which cannot be transferred between containers
After the conveyance arrives at the destination station, the device should be recovered by the destination, and stored and charged at the appointed place	Not applicable, it is embedded in the smart container
Transit (domestic): devices will flow among different supervision stations. Cross border one way supervision: devices will be recovered by the destination, and regularly carried back to the place of departure. Cross border two way supervision: device will be recovered after arriving at the destination, and returned via return vehicles to the launching point for recycling or re-use	Not applicable, it is embedded in the smart container

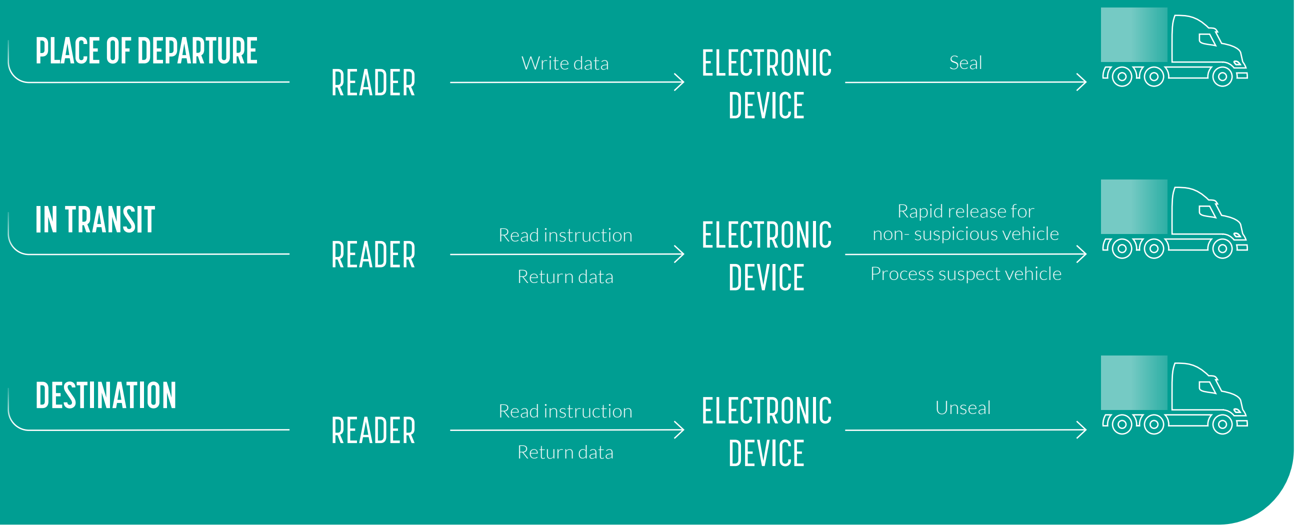
7.2 OPERATING PROCESS

I. OPERATING PROCESS OF PASSIVE DEVICES/SEMI-ACTIVE DEVICES

Handling

Devices are operated through readers at the place of departure, en route (including transit) and at the place of destination. Data is written at the place of departure, and read and verified en route and at the place of destination.

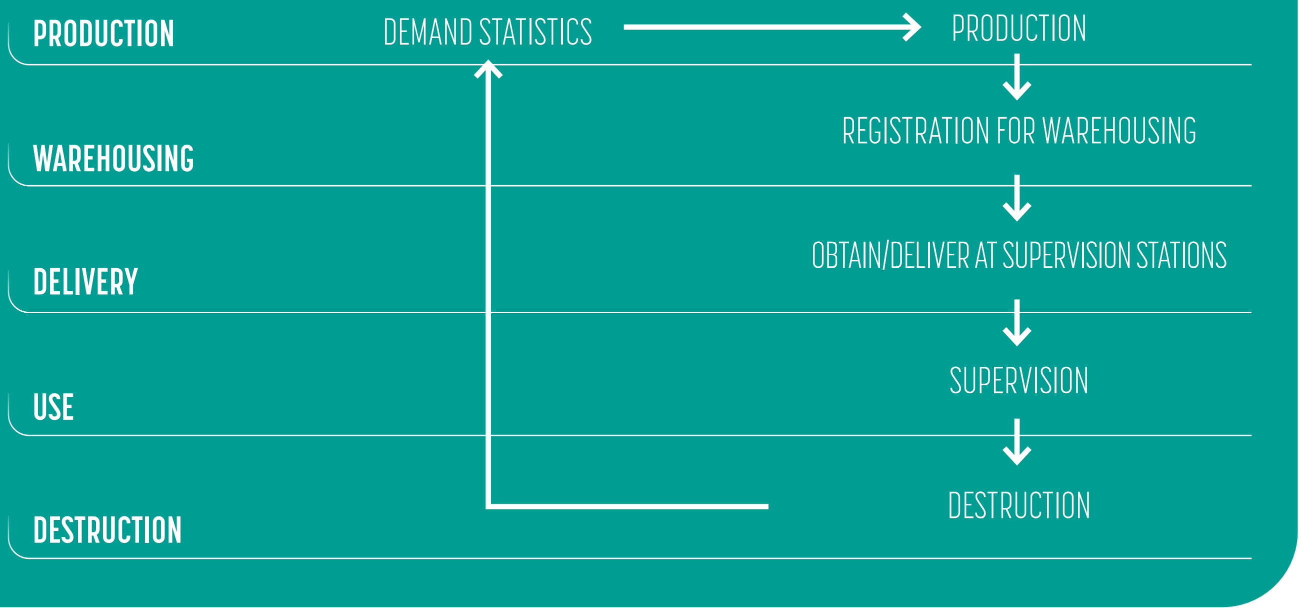
PASSIVE/SEMI-ACTIVE DEVICE PROCESSES



Storing

Device storage management includes the whole process from device production, to warehousing, registration, delivery, status tracking, and data statistics, etc.

PASSIVE/SEMI-ACTIVE DEVICE STORING PROCESSES



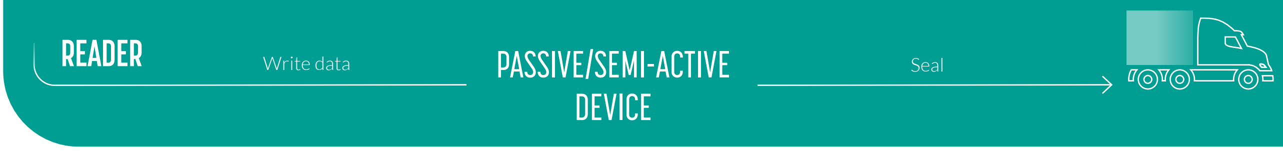
Sealing

Passive/semi-active devices are sealed in two steps:

Step 1: writing data; if a supervision platform is available, the correspondence to the vehicles or cargos shall be registered at the platform.

Step 2: locking the container or the cargo vessel through the mechanical locking function of the device.

PASSIVE/SEMI-ACTIVE DEVICE SEALING PROCESSES



READER

Write data

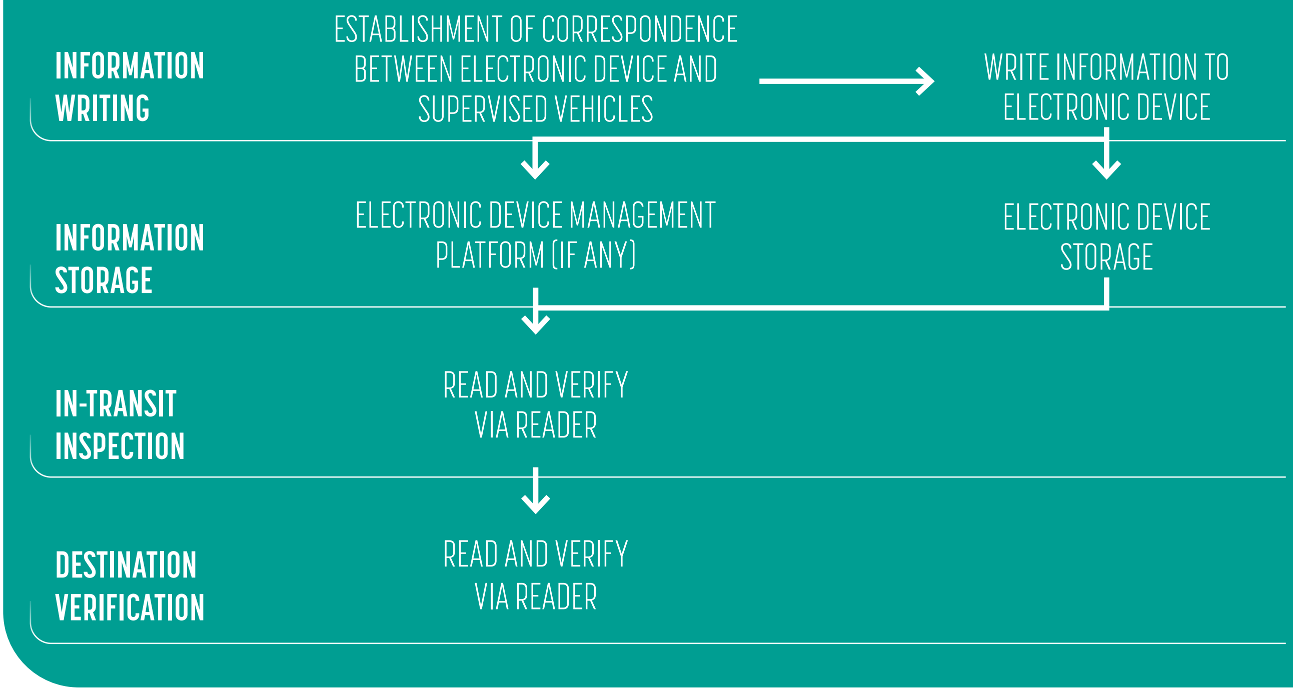
PASSIVE/SEMI-ACTIVE DEVICE

Seal

Data management and transfer

Due to the issue of storage capacity, passive/semi-active devices can only store a small amount of information (e.g. the ID of the related documents and the licence plate number). The supervision stations along the route and the destination can read the device information through a reader and verify the information as well.

PASSIVE/SEMI-ACTIVE DEVICES DATA MANAGEMENT AND TRANSFER PROCESSES



INFORMATION WRITING

ESTABLISHMENT OF CORRESPONDENCE BETWEEN ELECTRONIC DEVICE AND SUPERVISED VEHICLES

WRITE INFORMATION TO ELECTRONIC DEVICE

INFORMATION STORAGE

ELECTRONIC DEVICE MANAGEMENT PLATFORM (IF ANY)

ELECTRONIC DEVICE STORAGE

IN-TRANSIT INSPECTION

READ AND VERIFY VIA READER

DESTINATION VERIFICATION

READ AND VERIFY VIA READER

Monitoring

Real-time visual supervision cannot be carried out as passive/semi-active devices cannot actively report the information. However, information can be read at locations en route using readers.

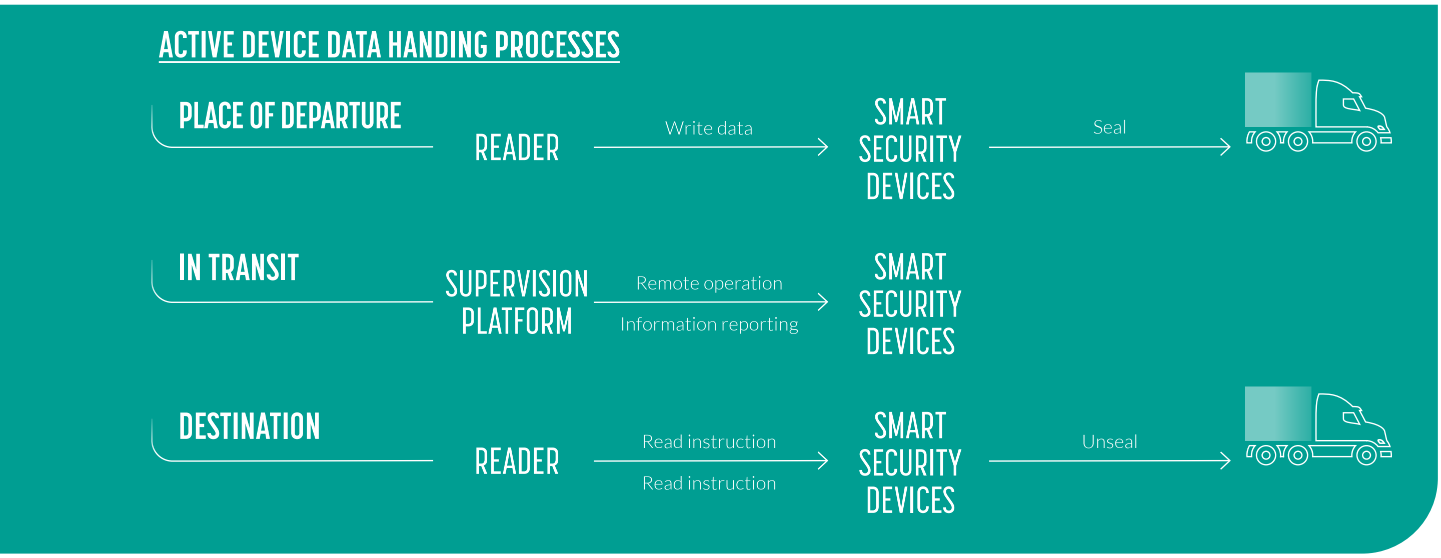
Alarm management

Passive/semi-active devices cannot report the position and status information, having only a single alarm. In addition, they can only verify illegal conveyance behaviour by verifying the consistency of the information through readers along the route and at the destination.

Operating process of active devices

Handling

Active devices are capable of short-distance operation through a reader or remote operation through a supervision platform.



ACTIVE DEVICE DATA HANDING PROCESSES

PLACE OF DEPARTURE

READER → Write data → SMART SECURITY DEVICES → Seal →

IN TRANSIT

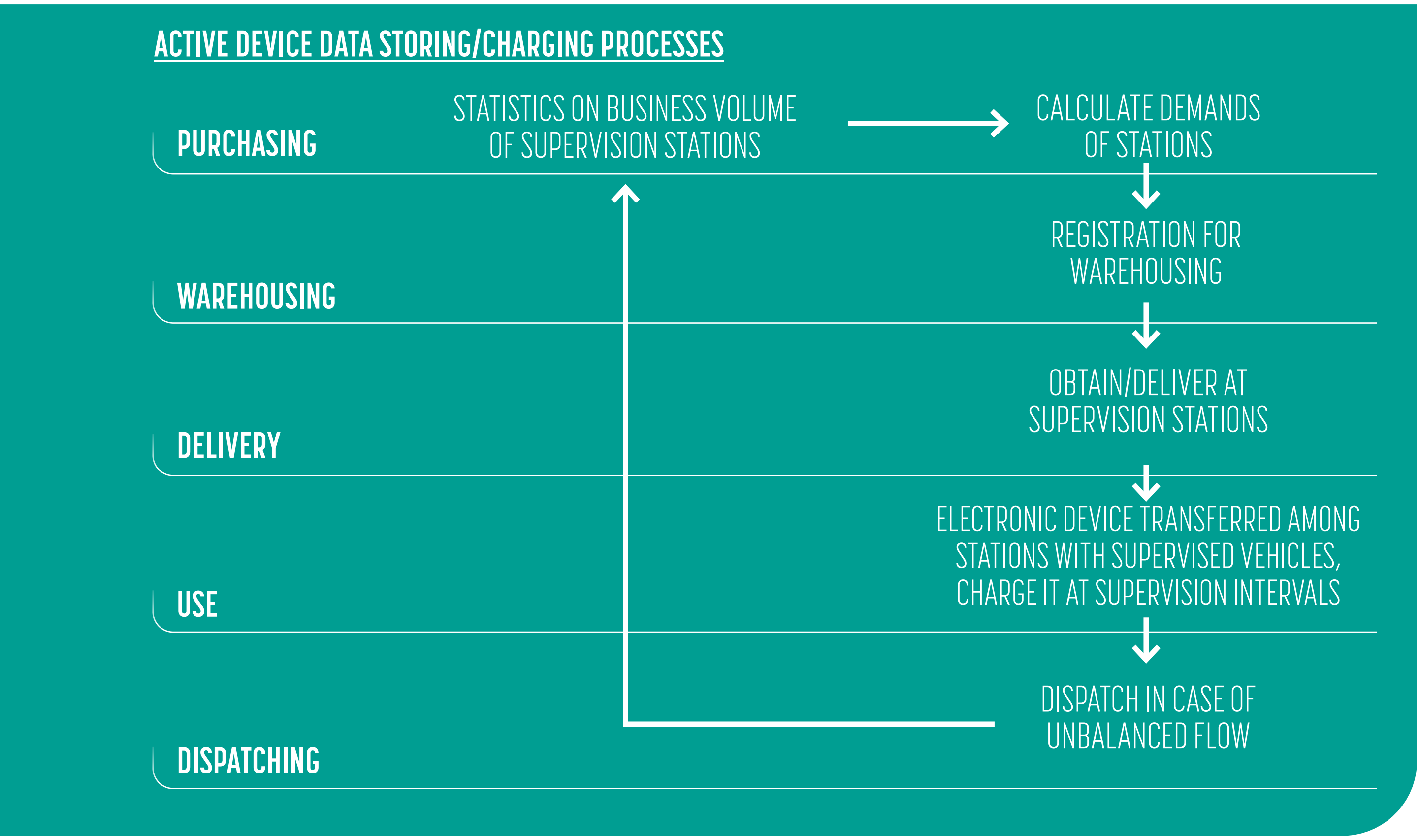
SUPERVISION PLATFORM → Remote operation / Information reporting → SMART SECURITY DEVICES

DESTINATION

READER → Read instruction / Read instruction → SMART SECURITY DEVICES → Unseal →

Storing/charging

Active devices are transferred and recycled among different stations. For the purposes of delivery and configuration, the business volume of supervision stations should be taken into consideration. A platform could be used for dispatching when devices are transferred among different stations.



ACTIVE DEVICE DATA STORING/CHARGING PROCESSES

PURCHASING: STATISTICS ON BUSINESS VOLUME OF SUPERVISION STATIONS → CALCULATE DEMANDS OF STATIONS

WAREHOUSING: REGISTRATION FOR WAREHOUSING

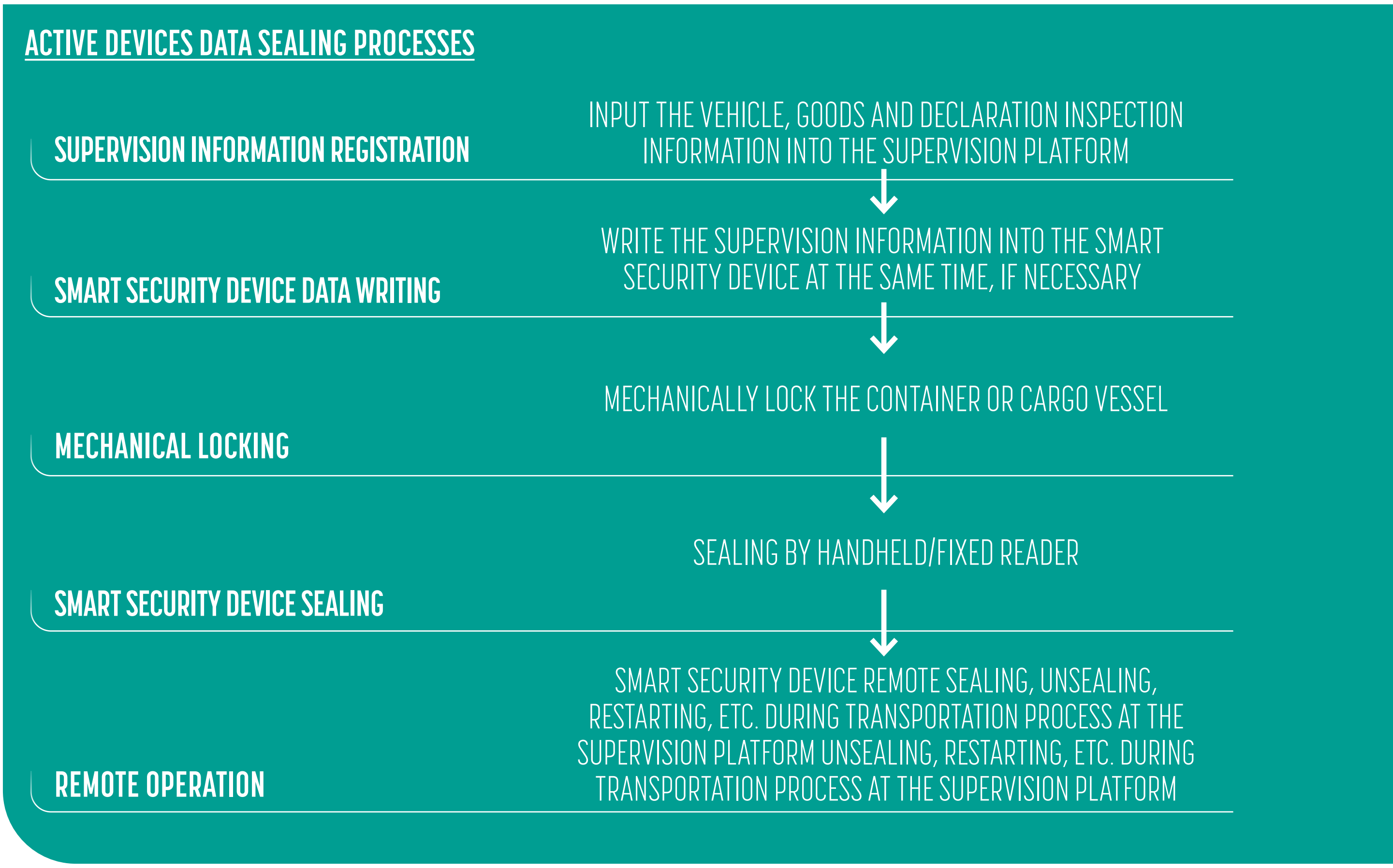
DELIVERY: OBTAIN/DELIVER AT SUPERVISION STATIONS

USE: ELECTRONIC DEVICE TRANSFERRED AMONG STATIONS WITH SUPERVISED VEHICLES, CHARGE IT AT SUPERVISION INTERVALS

DISPATCHING: DISPATCH IN CASE OF UNBALANCED FLOW

Sealing

The primary distinction between active and passive devices lies in the sealing process at the place of departure. Active devices are equipped with active reporting functionality, allowing real-time communication at any moment. This enables remote sealing, unsealing, and other operations as required during the journey, offering a more flexible operating mode.



ACTIVE DEVICES DATA SEALING PROCESSES

SUPERVISION INFORMATION REGISTRATION — INPUT THE VEHICLE, GOODS AND DECLARATION INSPECTION INFORMATION INTO THE SUPERVISION PLATFORM

SMART SECURITY DEVICE DATA WRITING — WRITE THE SUPERVISION INFORMATION INTO THE SMART SECURITY DEVICE AT THE SAME TIME, IF NECESSARY

MECHANICAL LOCKING — MECHANICALLY LOCK THE CONTAINER OR CARGO VESSEL

SMART SECURITY DEVICE SEALING — SEALING BY HANDHELD/FIXED READER

REMOTE OPERATION — SMART SECURITY DEVICE REMOTE SEALING, UNSEALING, RESTARTING, ETC. DURING TRANSPORTATION PROCESS AT THE SUPERVISION PLATFORM UNSEALING, RESTARTING, ETC. DURING TRANSPORTATION PROCESS AT THE SUPERVISION PLATFORM

Data management and transfer

Active devices boast significant storage capacity, enabling them to store comprehensive multi-dimensional information about the supervised object:

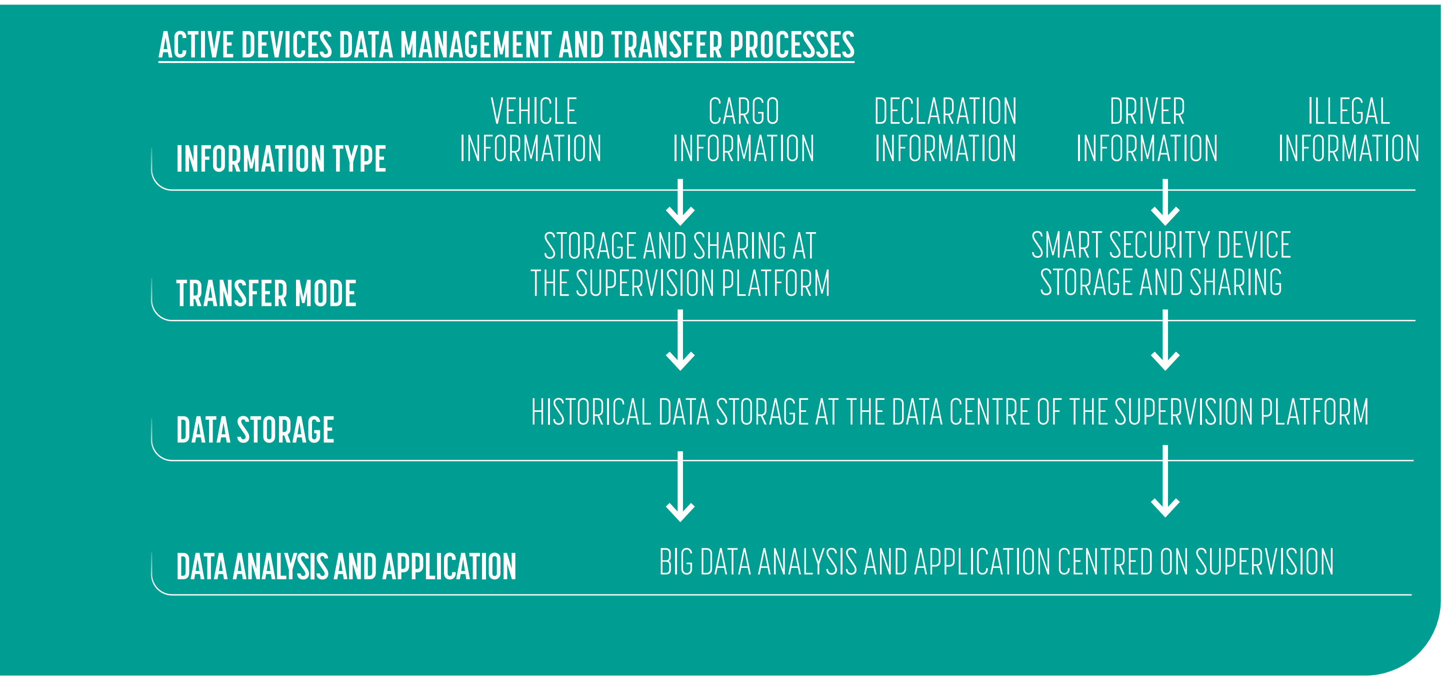
Vehicle information: licence plate number, vehicle model, specification (length, width and height), vehicle weight and container number.

Cargo information: cargo type, quantity, unit, place of origin, consignor and consignee.

Declaration information: Customs declaration number, manifest number and attached documents.

Driver information: nationality, name and contact number.

The above information is registered and stored in the smart security lock and can be accessed for reading through authorized devices, promoting the sharing of supervision data. Storing and analysing supervision data contributes to building a risk identification system. By promptly assessing the violation risk of the supervised object before departure and arrival, Customs officers can effectively prioritize supervision or facilitate quick release procedures.



ACTIVE DEVICES DATA MANAGEMENT AND TRANSFER PROCESSES

INFORMATION TYPE: VEHICLE INFORMATION, CARGO INFORMATION, DECLARATION INFORMATION, DRIVER INFORMATION, ILLEGAL INFORMATION

TRANSFER MODE: STORAGE AND SHARING AT THE SUPERVISION PLATFORM; SMART SECURITY DEVICE STORAGE AND SHARING

DATA STORAGE: HISTORICAL DATA STORAGE AT THE DATA CENTRE OF THE SUPERVISION PLATFORM

DATA ANALYSIS AND APPLICATION: BIG DATA ANALYSIS AND APPLICATION CENTRED ON SUPERVISION

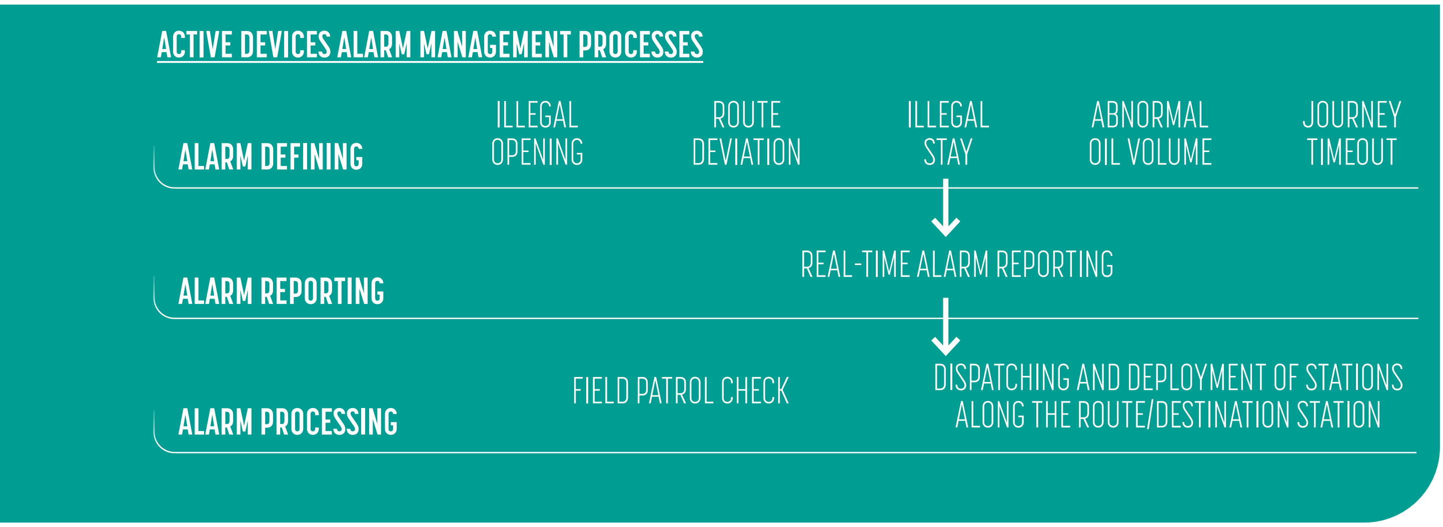
A. MONITORING

Active devices can report the position and status information about the supervised object in real time. The supervised vehicles can be subject to visual supervision through Geographical Information System (GIS) mapping.

The Customs officer can establish a supervision centre to have an intuitive understanding of the quantity, position, and normal and illegal quantity of supervised vehicles.

B. ALARM MANAGEMENT

Based on the information reported by the device, the supervision platform can define various types of alert events, such as route deviation, illegal stay, overtime stay, illegal opening, journey timeout and abnormal oil volume (oil tank truck). The Customs officer can deal with the alarms by different means on the basis of various type of alarm, including field checks, and dispatching and deployment at the destination.



ACTIVE DEVICES ALARM MANAGEMENT PROCESSES

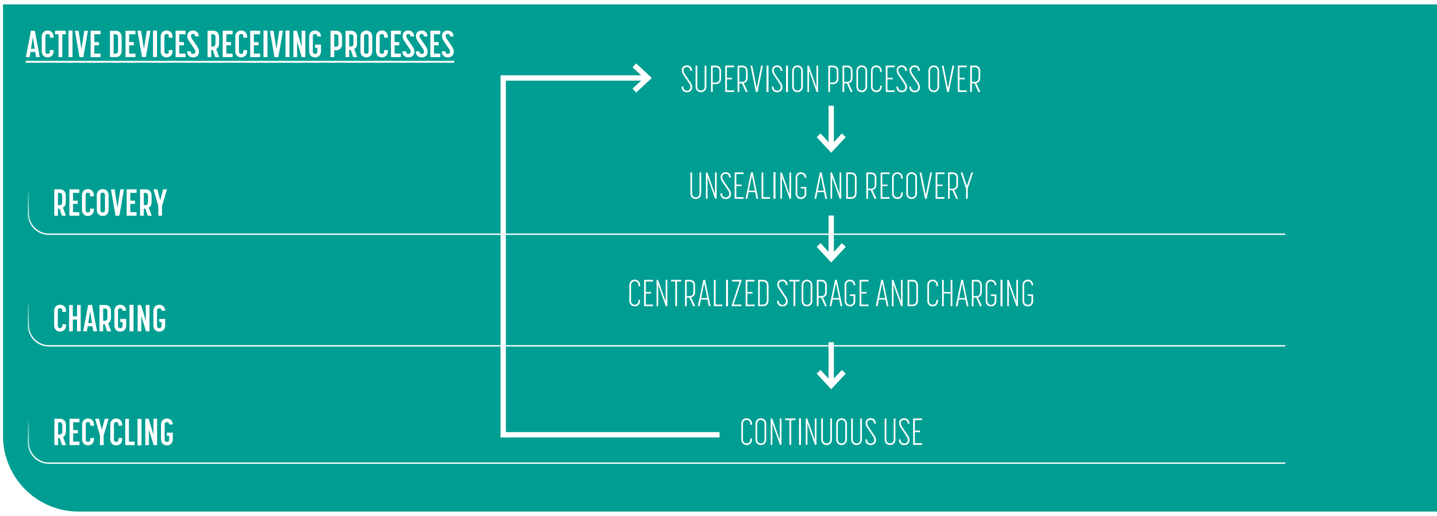
ALARM DEFINING: ILLEGAL OPENING, ROUTE DEVIATION, ILLEGAL STAY, ABNORMAL OIL VOLUME, JOURNEY TIMEOUT

ALARM REPORTING: REAL-TIME ALARM REPORTING

ALARM PROCESSING: FIELD PATROL CHECK; DISPATCHING AND DEPLOYMENT OF STATIONS ALONG THE ROUTE/DESTINATION STATION

C. RECEIVING

Active devices are commonly equipped with GPS and mobile communication modules, tailored to their specific applications. While the cost per use of smart security locks may be relatively higher compared to passive and semi-active devices, they offer the advantage of recyclability or reusability. This feature reduces the one-off use costs, necessitating a well-defined system with clear roles and responsibilities to manage the recycling or re-use process effectively.



ACTIVE DEVICES RECEIVING PROCESSES

RECOVERY

CHARGING

RECYCLING

SUPERVISION PROCESS OVER

UNSEALING AND RECOVERY

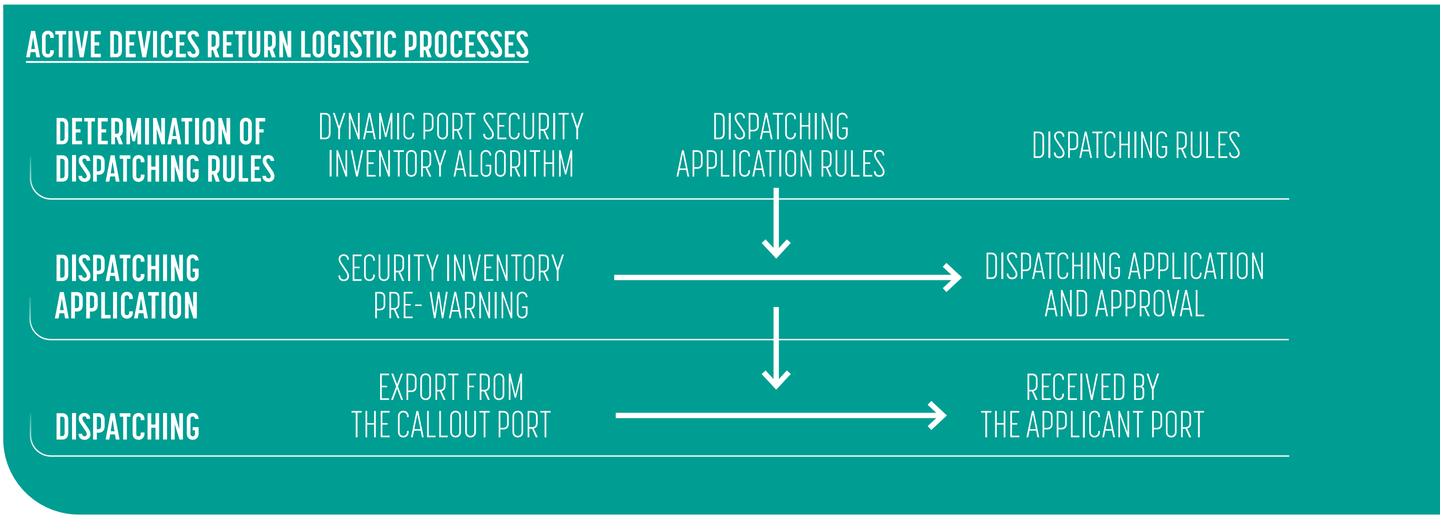
CENTRALIZED STORAGE AND CHARGING

CONTINUOUS USE

D. RETURN LOGISTICS

Following registration and delivery, active devices are transferred between different stations, which may result in an unbalanced distribution during operations. This unbalanced state can manifest as net inflow or net outflow. Net inflow occurs when many devices enter a station while only a few leave, causing an excessive accumulation of devices. Conversely, net outflow refers to a situation where many devices depart from a station while fewer devices are transferred from other stations, leading to a decrease in the number of devices at that station. This reduction in devices can hinder normal supervision operations at the affected station.

To address these issues, relevant stakeholders can develop an intelligent device dispatching mechanism based on port business volume. Additionally, it is advisable to establish a dynamic port security inventory utilizing a dispatching algorithm. This approach will enable timely transfer and dispatch of devices, ensuring smooth operations at each station.



ACTIVE DEVICES RETURN LOGISTIC PROCESSES

DETERMINATION OF DISPATCHING RULES

DYNAMIC PORT SECURITY INVENTORY ALGORITHM

DISPATCHING APPLICATION RULES

DISPATCHING RULES

DISPATCHING APPLICATION

SECURITY INVENTORY PRE- WARNING

DISPATCHING APPLICATION AND APPROVAL

DISPATCHING

EXPORT FROM THE CALLOUT PORT

RECEIVED BY THE APPLICANT PORT

CHAPTER 8

APPLICATION OF SSDs

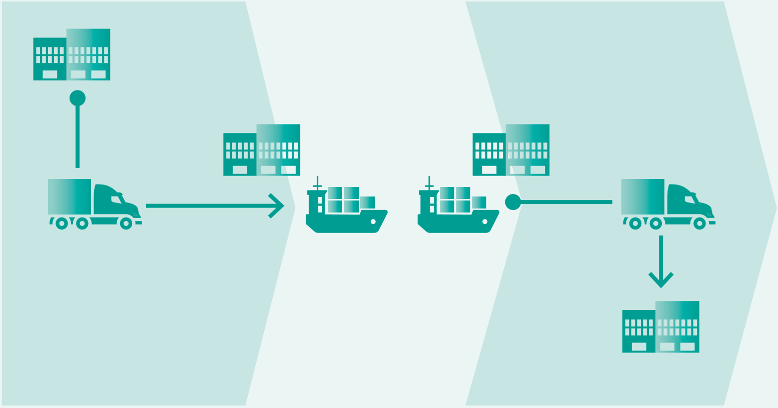
8

APPLICATION IN TRANSIT (DOMESTIC)

OVERVIEW OF CUSTOMS TRANSIT (DOMESTIC)

Transit (domestic) includes (a) a transit (import): transportation from a Customs office of entry to an inland Customs office for clearance; (b) a transit (export): transportation from an inland Customs office to a Customs office of exit; and (c) an internal transit: transportation from one inland Customs office to another inland Customs office.

THREE TYPES OF NATIONAL CUSTOMS TRANSIT



TRANSIT FOR EXPORTATION

transportation from an inland Customs office to an office of exit

TRANSIT FOR IMPORATION

transportation from an office of entry to an inland Custom office

INTERNAL TRANSIT

transportation from one inland Custom office to another inland Customs office

ROLE OF DEVICES IN CUSTOMS TRANSIT (DOMESTIC)

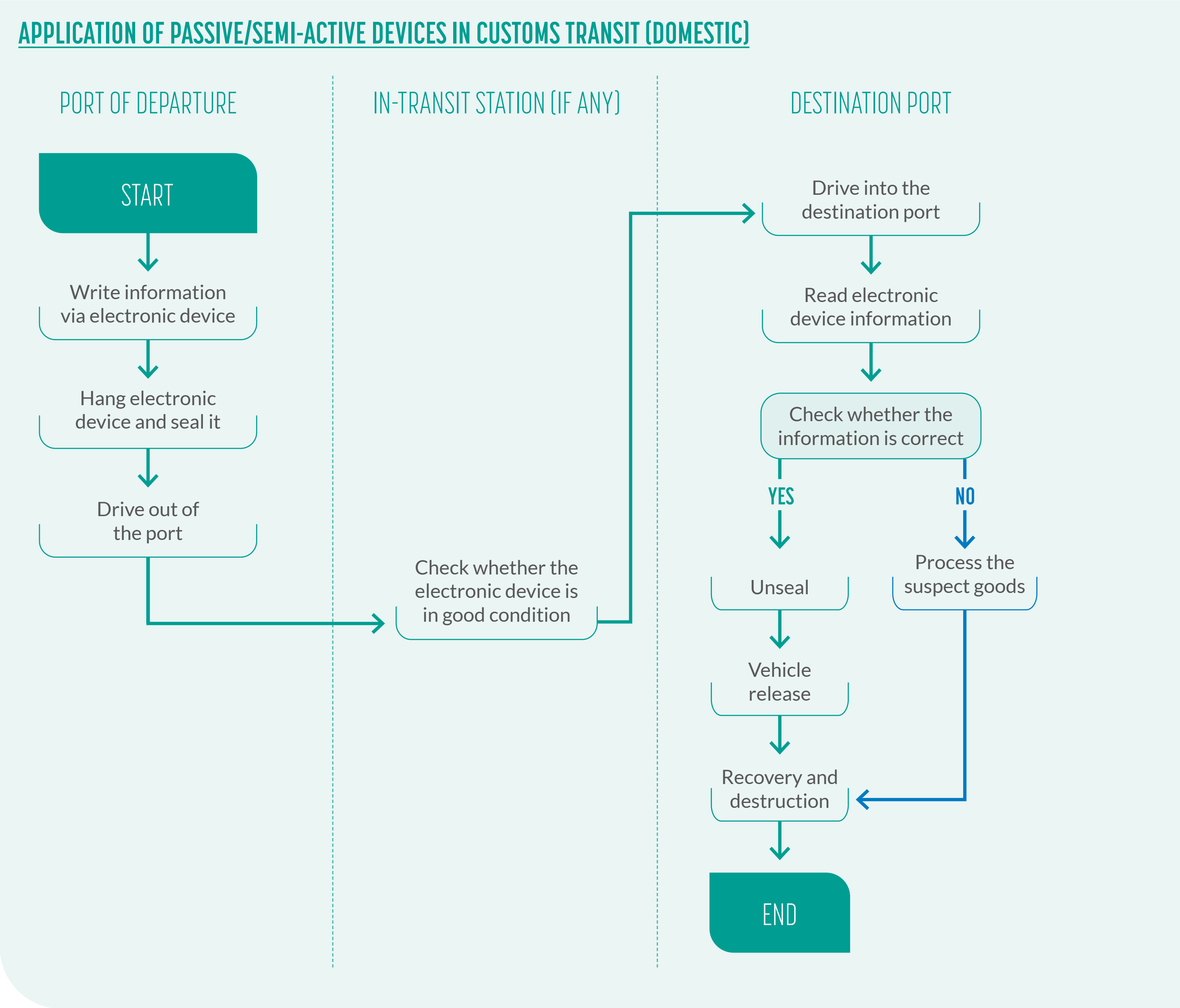
On the one hand, devices are employed in Customs transit (domestic) to ensure the following:

a. Customs at the departure station conduct checks on declaration information.

b. The cargo type, quantity, status, and other relevant details remain consistent during transportation until the cargo reaches the Customs site at the destination, following inspection or verification by Customs at the departure station. This helps prevent various illicit activities, such as smuggling.

On the other hand, the Customs office can expedite the release process for vehicles or cargo with no abnormal device status, thereby enhancing clearance efficiency.

APPLICATION PROCESS FOR PASSIVE/SEMI-ACTIVE DEVICES: FLOW DIAGRAM


APPLICATION OF PASSIVE/SEMI-ACTIVE DEVICES IN CUSTOMS TRANSIT (DOMESTIC)
PORT OF DEPARTURE
IN-TRANSIT STATION (IF ANY)
DESTINATION PORT
START
Write information via electronic device
Hang electronic device and seal it
Drive out of the port
Check whether the electronic device is in good condition
Drive into the destination port
Read electronic device information
Check whether the information is correct
YES
NO
Unseal
Process the suspect goods
Vehicle release
Recovery and destruction
END

DESCRIPTION

PROCESS AT THE PLACE OF DEPARTURE

Road:

1. Writing the supervision information through the device, such as licence plate number, document number, manifest number and container number, if necessary.
2. Mechanically locking the container or other cargo vessels with a device.
3. Driving the supervised vehicles out of the departure station.

Rail:

1. Writing the supervision information through the device, such as train number, container number and document number, if necessary.
2. Mechanically locking the train container with a device.
3. Driving the supervised vehicles out of the departure station.
4. Transmitting the Customs transit declaration form (including device information) to the place of transfer or the destination.

IN-TRANSIT SUPERVISION

Road:

1. Reading the tag with a reader, and ensuring that the device is in good condition.
2. Checking with the Customs transit declaration form to ensure that no unlawful intrusion has taken place.
3. Addressing suspicion or releasing.

Rail:

1. Reading SSD e-tag with a reader, and confirming good seal condition.
2. Checking with the Customs transit declaration form, and ensuring that no unlawful intrusion has taken place.
3. Addressing suspicion or releasing.
4. Mechanical unsealing, recovery, or destruction of the device.

PROCESS AT DESTINATION

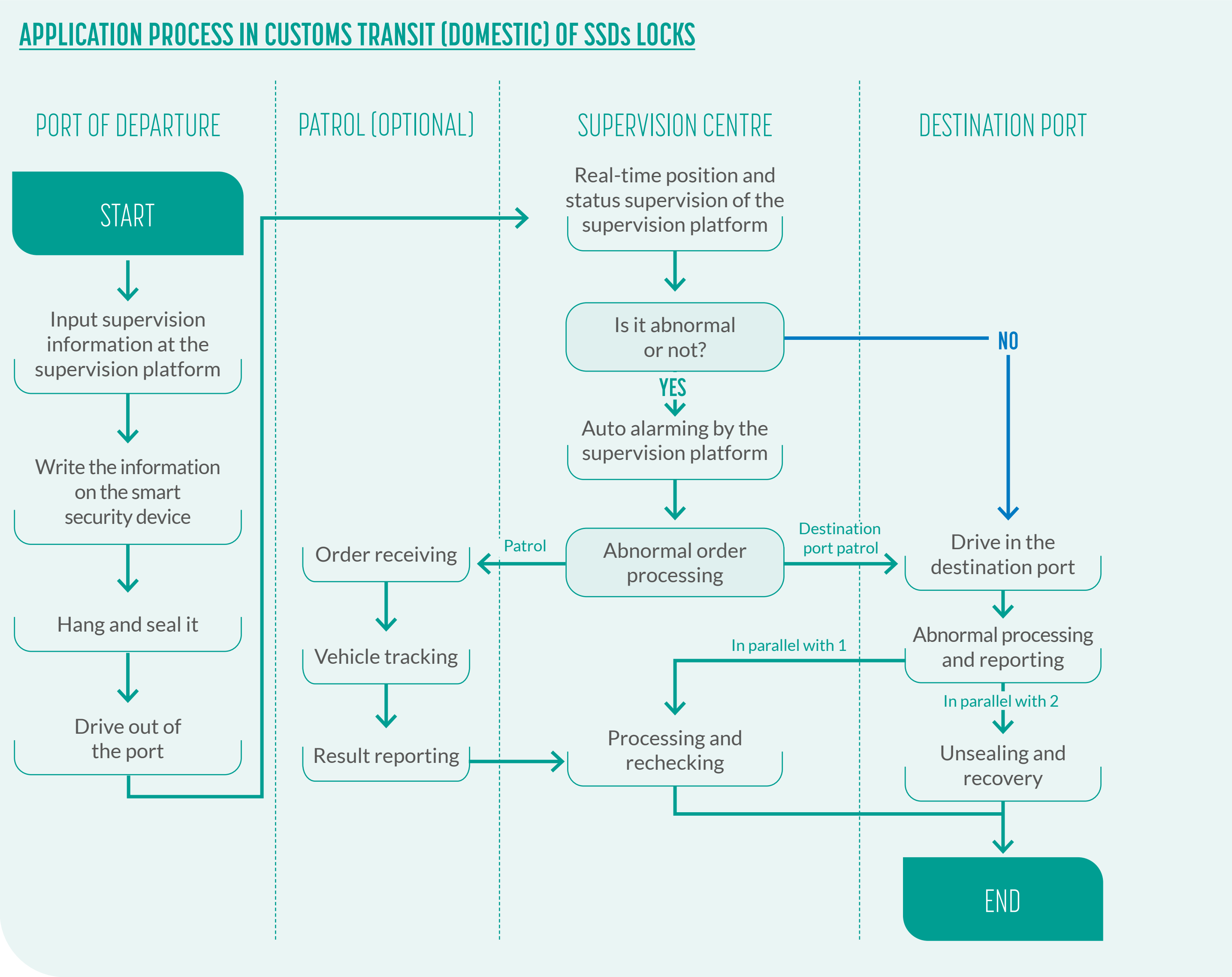
Road:

1. Reading the tag with a reader, and confirming that the device is in good condition.
2. Checking with the Customs transit declaration form and cancelling the Customs transit document after verification, if no unlawful intrusion has been noticed.
3. Addressing suspicion or release.
4. Mechanical unsealing, recovery, or destruction of the device.

Rail:

1. Reading the tag with a reader, and confirming that the device is in good condition.
2. Checking with the Customs transit declaration form and cancelling the Customs transit document after verification, if no unlawful intrusion has been noticed.
3. Addressing suspicion or release.
4. Mechanical unsealing, recovery, or destruction of the device.

APPLICATION PROCESS FOR ACTIVE DEVICES


APPLICATION PROCESS IN CUSTOMS TRANSIT (DOMESTIC) OF SSDs LOCKS

PORT OF DEPARTURE
PATROL (OPTIONAL)
SUPERVISION CENTRE
DESTINATION PORT
START
Input supervision information at the supervision platform
Write the information on the smart security device
Hang and seal it
Drive out of the port
Real-time position and status supervision of the supervision platform
Is it abnormal or not?
NO
YES
Auto alarming by the supervision platform
Abnormal order processing
Patrol
Destination port patrol
Order receiving
Vehicle tracking
Result reporting
Drive in the destination port
Abnormal processing and reporting
In parallel with 1
In parallel with 2
Processing and rechecking
Unsealing and recovery
END

DESCRIPTION

PROCESS AT THE PLACE OF DEPARTURE

Road:

1. Inputting the supervision information, including vehicle information, cargo information, driver's information, declaration information and inspection information.
2. Writing the supervision information into the active device, if necessary.
3. Hanging locking: mechanically locking the container or other cargo vessels.
4. Sealing with a reader or remotely via supervision platform.

Rail:

1. Inputting the supervision information, including train number information, container information, cargo information, declaration information and inspection information.
2. Writing the supervision information into the active device, if necessary.
3. Hanging locking: mechanically locking the container or other cargo vessels.
4. Sealing with a reader or remotely via supervision platform.

IN-TRANSIT SUPERVISION

Road:

1. The supervision centre can check the information about the vehicle position and status via supervision platform, and track it in real time.
2. An alarm is triggered in real time in the event of any illegal activities by the vehicle.
3. The supervision centre will process alarms, including a patrol check or dispatching and deployment at the destination. After receiving the inspection information, the patrol tracks the vehicles via the mobile app, and report the inspection results to the supervision centre. After receiving the dispatching and deployment information, the destination can well prepare for vehicle patrolling according to the instructions given by the supervision centre.

Rail:

1. The supervision centre can check the information about the vehicle position and status via the supervision platform, and track it in real time.
2. Alarm works in real time in the event of any illegal activities by the vehicle.
3. The supervision centre will process the alarms, including a patrol check or dispatching and deployment at the destination. After receiving the inspection information, the patrol tracks the vehicles via the mobile app, and report the inspection results to the supervision centre. After receiving the dispatching and deployment information, the destination can well prepare for patrolling of this train according to the instructions given by the supervision centre.

PROCESS AT DESTINATION

Road:

1. Driving the vehicles into the port.
2. Checking the device integrity and in-transit illegal alarms with a reader or via the supervision platform.
3. Inspecting or releasing based on the alarm grade.
4. Unsealing and recovering the device for sending to the appointed place for charging.

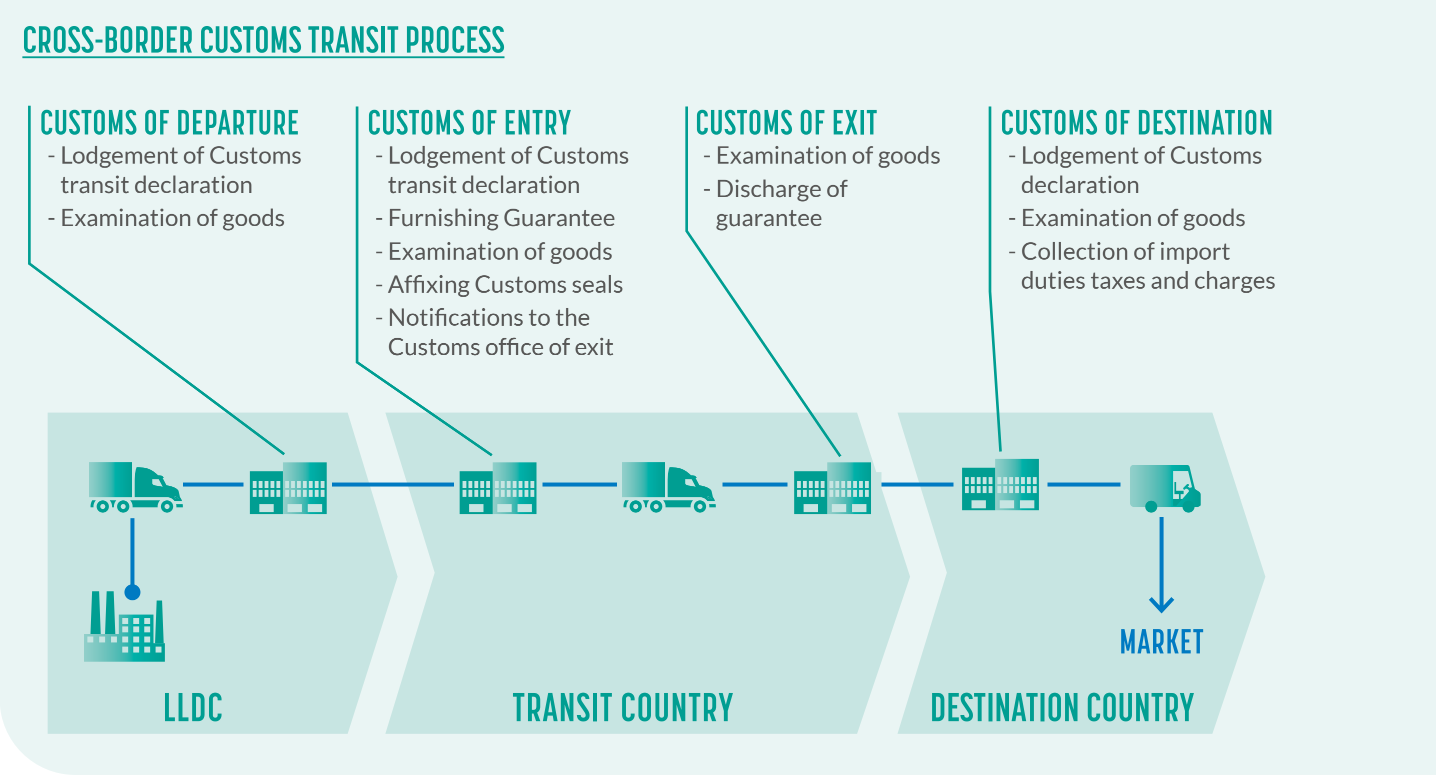
Rail:

1. Driving the vehicles into the destination station.
2. Unloading into the warehouse.
3. Checking the device integrity and in-transit illegal alarms with a reader or via the supervision platform.
4. Inspecting or releasing based on the alarm grade.
5. Unsealing and recovering the device for sending to the appointed place for charging.

APPLICATION IN CROSS-BORDER SUPERVISION

OVERVIEW OF CROSS-BORDER CUSTOMS SUPERVISION

Cross-border Customs supervision is designed for situations where cargo transportation requires crossing through other countries to reach the final destination, particularly in cases like LLDCs (Land Locked Developing Countries). In such instances, where there is no direct coastline, goods must be imported and exported through maritime countries. The international Customs transit process is illustrated in the following figure:



CROSS-BORDER CUSTOMS TRANSIT PROCESS

CUSTOMS OF DEPARTURE
- Lodgement of Customs transit declaration
- Examination of goods

CUSTOMS OF ENTRY
- Lodgement of Customs transit declaration
- Furnishing Guarantee
- Examination of goods
- Affixing Customs seals
- Notifications to the Customs office of exit

CUSTOMS OF EXIT
- Examination of goods
- Discharge of guarantee

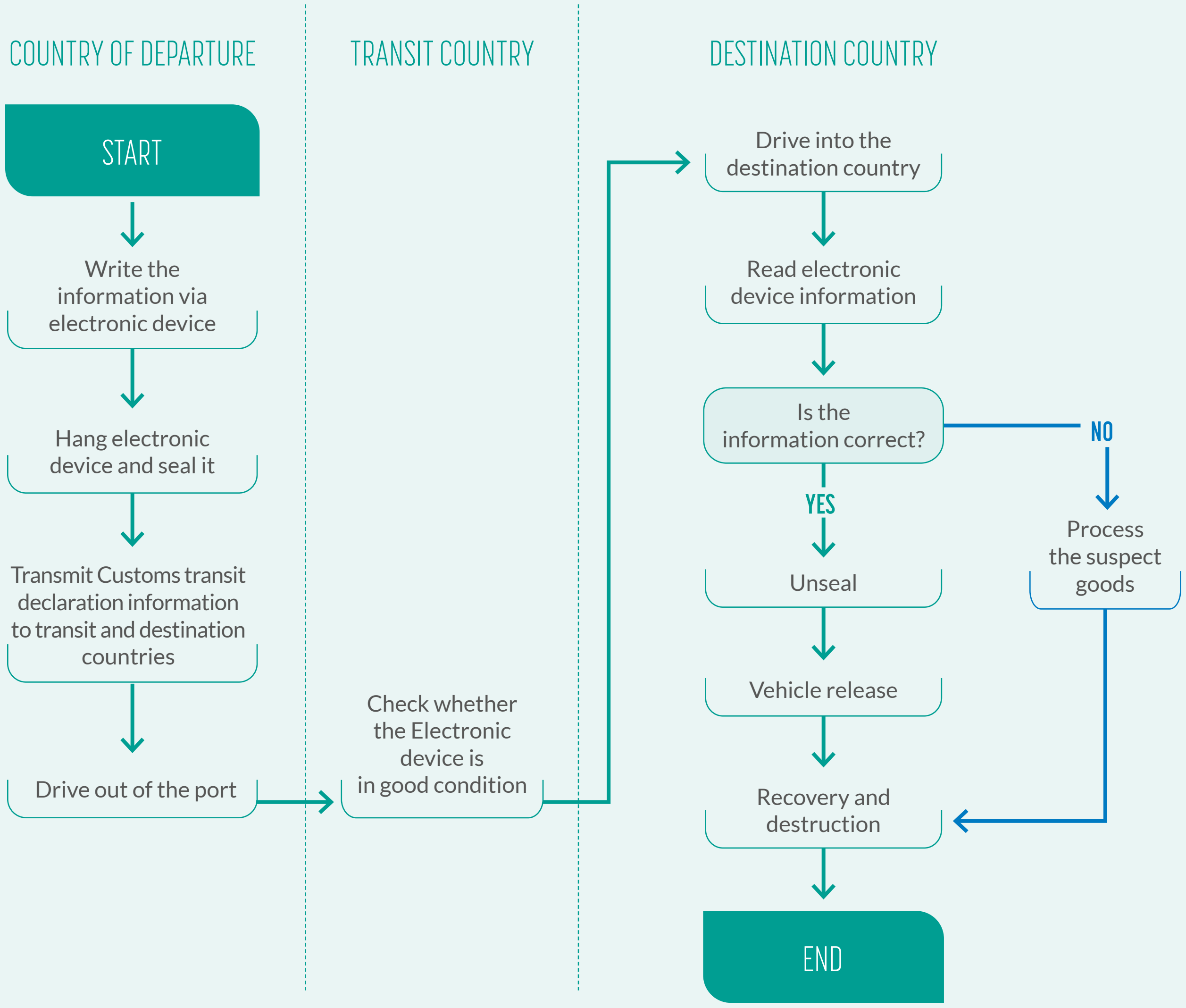
CUSTOMS OF DESTINATION
- Lodgement of Customs declaration
- Examination of goods
- Collection of import duties taxes and charges

Another typical application scenario for SSDs is cross-border trade. An exemplary case of this is the China Railway Express project undertaken by China, which exemplifies cross-border Customs transit services. This project has witnessed the operation of over 12,000 express trains, linking 56 domestic cities with 49 cities in 15 European countries.

ROLE OF SMART SECURITY LOCKS IN CROSS-BORDER CUSTOMS SUPERVISION

In cross-border supervision, devices can ensure cargo integrity from the place of departure to the destination country, keeping the cargo free from tampering, smuggling and entrainment, while the countries involved in the cross-border trade can establish mutually recognized supervision mechanisms, and achieve information sharing, mutual recognition of supervision and quick release through devices or a supervision platform. During the specific implementation process, the countries involved need to reach an agreement on relevant standards for devices.

APPLICATION PROCESS IN CROSS-BORDER CUSTOMS TRANSIT OF PASSIVE/SEMI-ACTIVE DEVICES



COUNTRY OF DEPARTURE
TRANSIT COUNTRY
DESTINATION COUNTRY
START
Write the information via electronic device
Hang electronic device and seal it
Transmit Customs transit declaration information to transit and destination countries
Drive out of the port
Check whether the Electronic device is in good condition
Drive into the destination country
Read electronic device information
Is the information correct?
NO
Process the suspect goods
YES
Unseal
Vehicle release
Recovery and destruction
END

DESCRIPTION

PROCESS IN THE COUNTRY OF DEPARTURE

Road:

1. Writing supervision information on a device, such as licence plate number, document number, manifest number and container number, if necessary.
2. Mechanically locking the container or other cargo vessels with a device.
3. Transmitting the Customs transit declaration information to the country of transit and to the destination country.
4. Driving the supervised vehicles out of the country of departure.

Rail:

1. Writing the supervision information on a device, such as train number, container number and document number, if necessary.
2. Mechanically locking the train container with a device.
3. Transmitting the Customs transit declaration form (including device information) to the place of transit or the destination.
4. Driving the supervised vehicles out of the country of departure.

MULTIMODAL

1. Completing the export declaration (to be done by the consignor or the multimodal transport operator) and sending the documents for Customs transit to the agency in the country of Customs transit.
2. Writing the supervision information on a device after Customs examination and inspection (if necessary), such as container number (maintaining the container unchanged in the transfer process), waybill number and cargo information.
3. Locking the containers with a device (to be done by Customs or the economic operator). Exporting the containers from the frontier port or transporting them from the domestic port to the frontier port for exporting.

PROCESS IN COUNTRY ALONG THE ROUTE

Road:

1. Reading the tag with a reader in the country of transit, and ensuring good seal condition.
2. Checking with the Customs transit declaration form, and ensuring no unlawful intrusion has taken place.
3. Addressing suspicion or release.

Rail:

1. Reading the device tag with a reader in the country of transfer, and confirming good seal condition.
2. Checking with the Customs transit declaration form, and ensuring no unlawful intrusion has taken place.
3. Addressing suspicion or release.

MULTIMODAL

1. Before the goods arrive transacting Customs clearance at the local Customs office (to be done by the consignor or the multimodal transport operator at the country of transit).
2. Inspecting device integrity (to be done by the Customs office), reading the device information with a reader, and checking it with the Customs transit declaration information.
3. Dealing with any suspect goods, and quickly releasing legitimate goods.

PROCESS IN DESTINATION COUNTRY

Road:

1. Reading the tag with a reader, and ensuring good seal condition.
2. Checking with the Customs transit declaration form, and discharging the Customs transit document after verification, if no unlawful intrusion has taken place.
3. Addressing any suspect goods, or release.
4. Mechanical unsealing, recovery, or destruction of the device.

Rail:

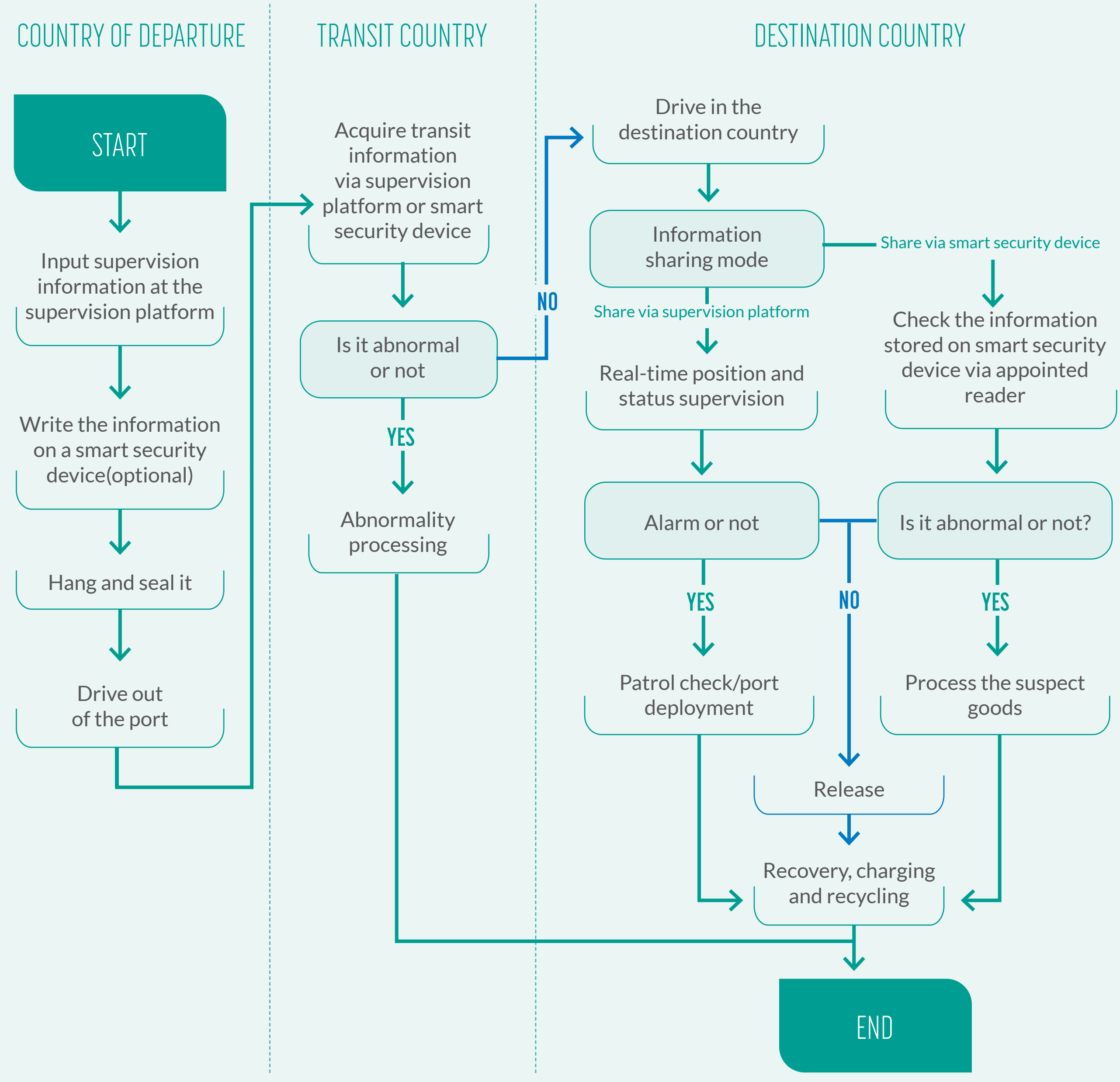
1. Reading the tag with a reader, and ensuring good seal condition.
2. Checking with the Customs transit declaration form, and discharging the Customs transit document after verification, if no unlawful intrusion has taken place.
3. Addressing any suspect goods, or releasing legitimate goods.
4. Mechanical unsealing, recovery, or destruction of the device.

MULTIMODAL

1. Before the goods arrive at the destination country, submitting the import declaration to the local Customs office (to be done by the consignor or the multimodal transport operator).
2. Upon the arrival of goods, inspecting the device integrity (to be done by the Customs office), reading the device information with a reader, and checking it the import declaration information.
3. Dealing with any suspect goods, and quickly releasing legitimate goods.
4. Mechanical unsealing, recovery, or destruction of the device.

APPLICATION PROCESS FOR ACTIVE DEVICES
FLOW DIAGRAM

APPLICATION PROCESS IN CROSS-BORDER CUSTOMS TRANSIT OF SSDs


COUNTRY OF DEPARTURE
TRANSIT COUNTRY
DESTINATION COUNTRY
START
Input supervision information at the supervision platform
Write the information on a smart security device(optional)
Hang and seal it
Drive out of the port
Acquire transit information via supervision platform or smart security device
Is it abnormal or not
NO
YES
Abnormality processing
Drive in the destination country
Information sharing mode
Share via smart security device
Share via supervision platform
Real-time position and status supervision
Check the information stored on smart security device via appointed reader
Alarm or not
Is it abnormal or not?
YES
NO
YES
Patrol check/port deployment
Process the suspect goods
Release
Recovery, charging and recycling
END

DESCRIPTION

PROCESS IN COUNTRY OF DEPARTURE

Road:

1. Inputting the supervision information, including vehicle information, cargo information, driver's information, declaration information and inspection information.
2. Writing the supervision information into the device, if necessary.
3. Hanging and locking: mechanically locking the container or other cargo vessels.
4. Sealing with a reader or remotely with a supervision platform.

Rail:

1. Inputting the supervision information, including train number information, container information, cargo information, declaration information and inspection information.
2. Writing the supervision information into the device, if necessary.
3. Hanging and locking: mechanically locking the container or other cargo vessels.
4. Sealing with a reader or remotely with a supervision platform.

MULTIMODAL

1. Completing the export declaration (to be done by the consignor or the multimodal transport operator) and sending the documents for Customs transit to the agency in the country of Customs transit.
2. Writing the supervision information (such as container number, waybill number and cargo information) on the device after Customs examination and inspection (if necessary), scanning relevant documents, checking the images, storing in the device, and recording the above information on the supervision platform.
3. Locking the containers via the device (to be done by the Customs office). Exporting the containers from the frontier port or transporting them from the domestic port to the frontier port for exporting.
4. When exporting from inland ports, the country of origin shall use the supervision platform for in-transit supervision. The device will report the position and status information in real time, and trigger an alarm automatically in case of illegal behaviours. The Customs office will check and take appropriate action based on such alarms. If no illegal behaviour is noted after arrival at the border port, the goods will be released quickly.

SUPERVISION BY COUNTRIES ALONG THE ROUTE

Road:

1. If a unified supervision platform is established by the regional countries, checking, by the countries along the route, the real-time vehicle position, status and track information and related Customs transit declaration information through the supervision platform. If no unified supervision platform is available, carrying out, by the countries along the route, information sharing and mutual recognition using information stored in the device.
2. Vehicles found to have carried out illegal activities shall be dealt with in accordance with the relevant laws.
3. If no illegal behaviour is noted, vehicles will not be rechecked. Instead, the vehicles shall be released quickly.

Rail:

1. If a unified supervision platform is established, national supervision centres of the countries along the route can check the real-time vehicle position, status and track information through the supervision platform.
2. Vehicles found to have carried out illegal activities shall be dealt with in accordance with the relevant laws.
3. If no illegal behaviour is noted, vehicles will not be rechecked. Instead, the vehicles shall be released quickly.

MULTIMODAL

1. Before goods arrive at the country of transit, conducting Customs clearance at the local Customs office (to be done by the Consignor or the multimodal transport operator).
2. If a supervision platform is available for the countries along the route: acquiring the supervised cargo information through the supervision platform and checking it against the declaration information for in-transit supervision; the device will report the position and status information in real time, and trigger an alarm automatically in the event of illegal behaviours. Customs will check and take appropriate action based on such alarms. If no illegal behaviour is noticed, the goods will be released quickly.

   If a supervision platform is not available for the countries along the route: acquiring the supervised cargo information through the device, checking it against the declaration information, and inspecting, via a reader, the integrity of the device and any illegal behaviours in the transportation process.
3. Dealing with the suspect goods, quickly releasing non-suspicious goods, and carrying out mutual recognition of supervision.

PROCESS AT DESTINATION COUNTRY

Road:

1. Driving the vehicles into the port.
2. If a unified supervision platform is established by countries along the route, checking alarms in the transportation process through the supervision platform, and checking the real-time alarms of the supervision platform by patrolling; if no unified supervision platform is available, the countries along the route can carry out information sharing and mutual recognition by the supervision information stored in the device.
3. Inspecting or releasing based on the alarm grade.
4. Unsealing and recovering smart security locks for sending to the appointed place for charging.

Rail:

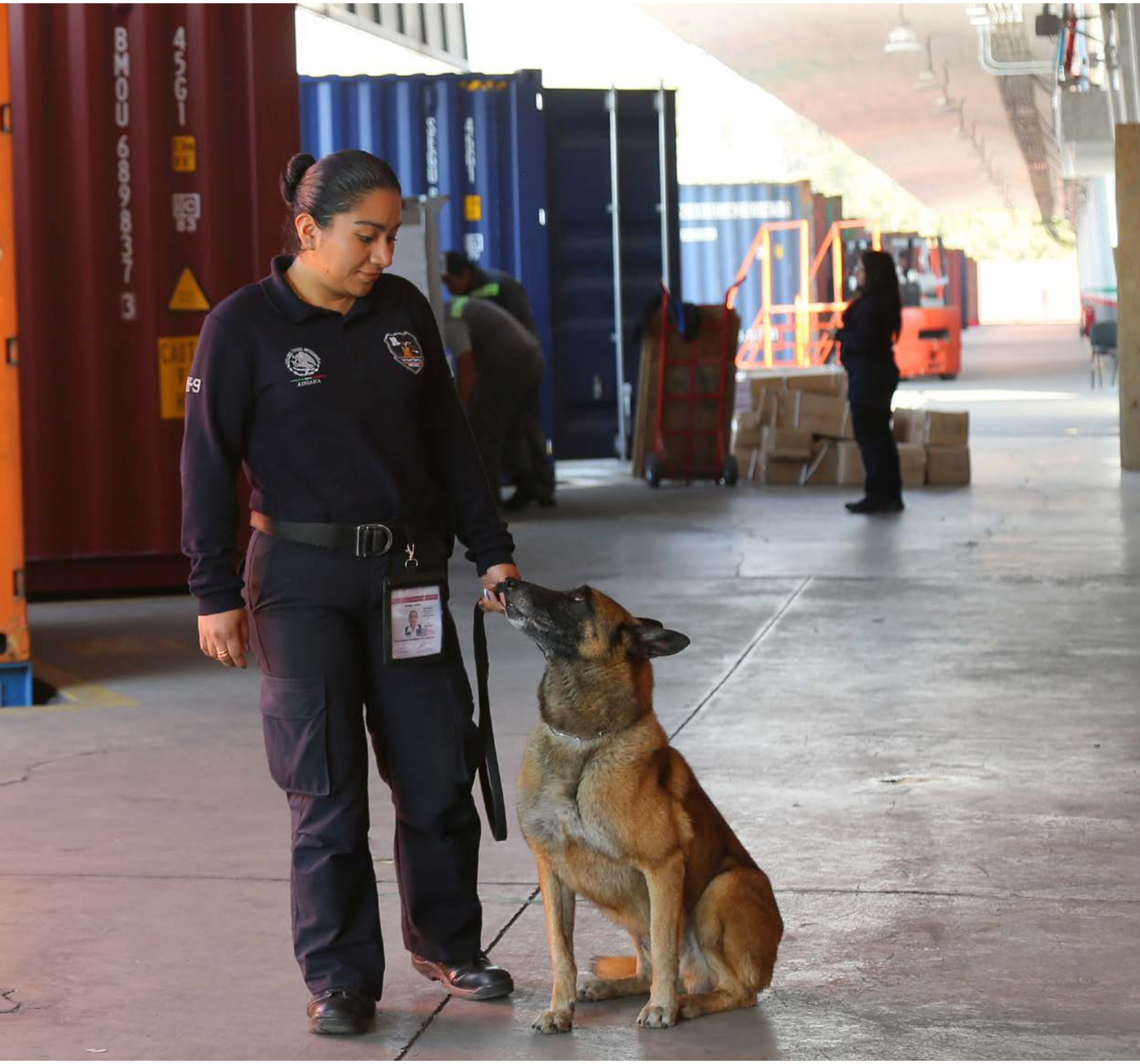
1. Driving the vehicles into the destination station.
2. Unloading into the warehouse.
3. If a unified supervision platform is established by countries along the route, checking illegal alarms in the transportation process through the supervision platform, and checking the real-time alarms of the supervision platform by patrolling; if no unified supervision platform is available, the countries along the route can carry out information sharing and mutual recognition by the supervision information stored in the device.
4. Inspecting or releasing based on the alarm grade.
5. Unsealing and recovering smart security locks for sending to the appointed place for charging.

MULTIMODAL

1. Before goods arrive at the country of transfer, submitting the import declaration to the local Customs office (to be done by the Consignor or the multimodal transport operator).
2. If a supervision platform is available in the destination country: acquiring the supervised cargo information through the supervision platform and checking with the declaration information for in-transit supervision; the device will report the position and status information in real time, and trigger an alarm automatically in the case of illegal behaviours. The Customs office will check and proceed accordingly. If no illegal behaviour is noted after arriving at the border port, the goods will be released quickly.

If no supervision platform is available in the destination country: acquiring the supervised cargo information through the device, checking with the declaration information, and inspecting, via reader, the SSD's integrity and illegal behaviours during the transportation process.

3. Addressing the suspect goods, quickly releasing non-suspicious goods, and realizing mutual recognition of supervision.
4. Unsealing, recovering and returning the device to the place of origin through logistics, or returning to the place of origin by supervising the return of the device.



CHAPTER 9

LEGAL AND PROCEDURAL FRAMEWORK

9

9.1 STAKEHOLDERS' LEGAL RIGHTS AND RESPONSIBILITIES

SSDs are gaining increasing traction globally as trade facilitation and security become more critical. While the application of SSDs brings substantial benefits, it can also lead to challenges and potential disputes related to data ownership, right to use, and the operation and maintenance of software and hardware during the transportation process. Devices also need to be sufficiently secure from intentional tampering, hacking attempts, infiltration, and substitutions with counterfeit components. To address these issues, it is essential to establish comprehensive laws and regulations that outline the roles, responsibilities, and rights of various entities and stakeholders involved.

Countries should enact laws, regulations, and rules, along with standardized documents, to precisely define the scope of rights and responsibilities, as well as provide clear definitions for the application of smart security devices. In the context of cross-border and cross-region transportation, bilateral and multilateral agreements established under WCO instruments and tools should be utilized to facilitate the widespread use of smart security devices in cross-border logistics.

To achieve clarity, it is imperative to define the legal rights and responsibilities of Customs, economic operators, site operators, carriers, consignees, consignors, freight forwarders, and other administrations involved in ports. Below is a brief outline, provided as an example:

CUSTOMS

The regulatory powers and responsibilities of Customs administrations with respect to the application of SSDs in cross-border and cross-region transportation should be stipulated. Customs administrations may consider providing trade facilitation measures on clearance in cases where SSDs are applied, based the device integrity and risk assessment. Common standards for the application of SSDs and associated equipment in cross-border and cross-region transportation should be established. For data generated during cross-border and cross-region transportation, storage and safety methods should be established. In the event of device abnormalities that may have occurred during cross-border and cross-region transportation, Customs should tackle these in accordance with national/regional laws and regulations.

A coordination mechanism and contingency plan should be established between the Customs administrations of each country for the regulation and management of SSDs.

ECONOMIC OPERATORS

Two types of economic operators exist in this context – those who provide the SSDs and related value-added services, and those who utilize them. It is crucial to establish clear legal rights and responsibilities for economic operators offering and using SSDs and related services in cross-border and cross-region transportation. Doing so will enable Customs administrations to effectively fulfil their regulatory duties.

Device operators should establish measures to ensure the provision of comprehensive services, to ensure confidentiality and security and to resolve accidents.

SITE OPERATORS

The legal status of site operators on the application of SSDs and associated equipment, defined as those operators overseeing the warehousing of imported and exported goods and their transfer, should be clearly defined. Site operators should ensure that the site fully supports the application and operation of SSDs, have at their disposal methods that allow data exchange with Customs to ensure data validity, and establish a contingency plan for tackling abnormalities and accidents.

CARRIERS

The legal rights and responsibilities of carriers on the application of SSDs in cross-border and cross-region transportation should be stipulated. Carriers that apply SSDs in cross-border and cross-region transportation should benefit on the entry of the goods and on Customs clearance.

Carriers should follow Customs regulations during transportation and ensure that SSDs will not be unsealed unexpectedly. Damages caused by force majeure and other abnormalities during transportation should be reported to Customs in a timely manner.

FREIGHT FORWARDERS, CONSIGNEES AND CONSIGNORS

The legal rights and responsibilities of freight forwarders, consignees and consignors on the application of SSDs in cross-border and cross-region transportation should be stipulated. Where required, freight forwarders, consignees and consignors should make declarations and go through relevant procedures following the Customs regulations on SSDs.

Freight forwarders, consignees and consignors that apply smart security locks in cross-border and cross-region transportation may enjoy benefits on Customs clearance, including when making declarations and going through relevant procedures.

OTHER PORT ADMINISTRATIONS

In order to enhance trade facilitation, other port administrations can share the data generated by SSDs with Customs for specified purposes. The results of law enforcement conducted by Customs administrations across borders in relation to the application of SSDs can be mutually recognized.

Stakeholders' responsibilities within the procedural framework (Solely intended as an example. The experiences can differ across countries)

CUSTOMS AT THE PLACE/COUNTRY OF DEPARTURE

Customs at the place/country of departure are responsible for accepting and processing declarations from consignees and consignors, Customs brokers, freight forwarders and carriers, supervising the sealing of SSDs on containers, checking documents and cargo to issue permits for the means of transportation to leave the Customs control area, and sending relevant information to Customs in transit countries and Customs at the country of destination.

CUSTOMS IN CHARGE OF SUPERVISION EN ROUTE AND CUSTOMS IN TRANSIT COUNTRIES

Customs in charge of supervision en route and Customs in transit countries are responsible for supervising containers with SSDs in accordance with their laws and regulations, contacting relevant parties to handle abnormalities detected during supervision and checking the results of handling. In the case of countries with a patrol team, after receiving alarms and notifications of abnormalities, the patrol team should track the vehicle, tackle the abnormality and revert.

CUSTOMS AT THE PLACE/COUNTRY OF DESTINATION

Customs at the place/country of destination are responsible for verifying the cargo arrival status and SSD integrity, unsealing the device and deciding on whether to inspect or release based on a risk assessment, business information, lock status, supervision en route and any alarm information recorded. For those that have applied SSDs, inspection-free passage, quick release and other measures providing facilitation at clearance can be offered.

CARRIERS

Carriers are responsible for filing records based on the regulations of each country. Carriers should declare information on the cargo carried by the means of transportation to Customs truthfully, move the cargo in accordance with the Customs regulations of each country and to the extent they are able, and ensure SSDs are not unsealed/tampered with at various stages of transportation. When detecting any abnormality during transportation, carriers should contact Customs in a timely manner and take necessary steps in accordance with Customs and related laws and regulations.

SITE OPERATORS

Site operators are responsible for providing a space to carry out sealing, unsealing, removal and other activities with respect to SSDs, as well as a working space for Customs, economic operators and other relevant parties, providing electricity, an internet connection and other infrastructure to ensure site operation, and the necessary assistance to Customs in handling emergencies.

CONSIGNEES CONSIGNORS AND FREIGHT FORWARDERS

Consignees, consignors and freight forwarders are responsible for declaring the goods to Customs truthfully, commissioning carriers for goods transportation and responding to common incidents during transportation such as Customs inspection and abnormalities.

OTHER PORT ADMINISTRATIONS

Within a legal framework, other port administrations can share the data generated by SSDs, such as location information, with Customs. In order to enhance trade facilitation, results of law enforcement by the two Customs administrations in relation to the application of SSDs can be mutually recognized.

9.2 DATA STORAGE AND SECURITY

During cross-border cargo transport, security issues have arisen in relation to the storage and transfer of data, as the Customs administrations of each country involved need to transfer large amount of data across borders, and many countries around the globe have established laws to protect personal data.

Unlike mechanical seals, SSDs have a data storage function. The body of the device exists only as a storage media, the data stored inside it is the key. Data security not only involves protection of personal information and privacy, but also covers commercial information.

Therefore, it is critical to have a comprehensive and stable legal framework for data storage and security. Once data has been stored, authorization and a licence are required to write additional data and read the stored data, due to data ownership rules.

Data security demands equal attention at all stages of a SSD's operation - when it is being written, in storage, and being read. Regardless of the data's current state, there is always a risk of it being leaked, stolen, or lost. While SSDs provide an added layer of protection for cargo, they can also become targets for theft and other criminal activities. The loss of smart security locks and the data they contain poses risks to Customs, traders, and other stakeholders involved.

To ensure data security, it is essential to develop legal safeguards, comprehensive instructions and guidance on the various technologies used in manufacturing SSDs, as well as to establish product quality standards. Manufacturers must adhere to the relevant regulations and standards during the production of SSDs and in the context of any post-production, maintenance, repairs, updates or other services provided. Users, including Customs, traders, and carriers, should only utilize SSDs that meet the specified standards.

For instance, the SSDs must have a secured storage component and a secured confidential information component. These requirements have been integrated into relevant product standards to enhance data security measures.

9.3 SECURITY REQUIREMENTS ON DATA STORAGE DEVICE

SSDs should normally meet (but are not limited to) the security requirements listed below:

a. Tamper resistance: sealing and unsealing of SSDs should be conducted with tamper resistance device.

b. Security verification: security verification of the registered body of SSDs should be conducted before sealing and unsealing.

c. Access control: access control should be applied on sealing and unsealing of SSDs.

d. Encrypted communication: information related to the process of security verification and access control should be transferred under encryption.

e. System security: security and protection measures should be applied to information transferred between SSDs, readers and back-end systems based on the information security level.

f. Secured record audit: sealing and unsealing of SSDs should be recorded and audited.

Security configuration and functions of SSDs should normally meet the requirements listed below, as examples:

a. SSDs should have the ability to generate asymmetric key pairs (sm2) for key-agreement protocols.

b. SSDs should be equipped with a secured storage component for the storage of key pairs.

c. SSDs should be equipped with a secured confidential information components to interact with information from the reader.

Readers include handheld readers and fixed readers; both types should normally meet the product function requirements on listed below, as examples:

a. There should be an exclusive identification number stored in each reader in advance, which cannot be changed.

b. Readers should have the ability to generate asymmetric key pairs (sm2) for key-agreement protocols.

c. Readers should be equipped with secured storage component for the storage of key pairs.

d. Readers should be equipped with a secured confidential information component to interact with information from SSDs and the registration system.

e. Readers should have a security verification mechanism of the required security standard.

f. All data transferred between readers and SSDs should be encrypted before transmission, where there is confidential information involved, to ensure the data security of the reader, the host computer and the back-end system.

Data stored in SSDs, such as images and manifest, should meet the product function requirements listed below, as examples:

a. The process of turning on/off the SSD data storage function should comply with the communication rules under the asymmetric key-agreement protocol between the reader and the smart security lock.

b. For data stored in SSDs, the md5 message-digest algorithm should be adopted to check the file integrity and avoid tampering.

Passive/semi-active devices should meet the product function requirements listed below, as examples:

a. Passive/semi-active devices can only be written with data once.

b. Communication between readers should be encrypted.

c. A password is required to read the data.

d. Once the device is broken, information stored inside automatically becomes unreadable or invalid.

SECURITY REQUIREMENTS ON DATA TRANSFER

When transferring data, encryption should be applied based on risk evaluation. When selecting and applying an encryption method, the rules listed below as examples could be followed:

a. The encryption method must comply with the relevant laws and regulations of the country. In cross-border and international trade, a common harmonized standard or practice may be necessary.

b. The type and feature of encryption algorithm and the length of cryptographic key should be decided in accordance with the level of protection, which will be based on risk assessment results.

c. General confidential information and critical confidential information should both be encrypted during storage and transfer. In this regard, two approaches could be adopted: symmetric encryption and asymmetric encryption or other suitable encryption advanced developments.

d. During the transfer of general confidential information and critical confidential information, digital signatures should be used to ensure the information is correct; use of digital signatures should comply with the following principles, as examples:

    I. The confidentiality of private keys should be fully protected to prevent the signature of cryptographic keyholders from being stolen.

    II. Security measures should be adopted to protect the integrity of public keys, for example, use of public key certification.

III. The type and feature of signature algorithms and length of cryptographic keys need to be confirmed.

IV. The cryptographic key used on digital signatures should be different from the one used on content encryption.

9.4 REQUIREMENTS WHEN CHANGING THE DATA SECURITY LEVEL

The data security level needs to be enhanced constantly. The security level of general data needs to be updated by the owner of the data or the owner's service provider. The category will then be adjusted accordingly and the people in charge of information security will be informed of the change and record it on file. The data security level should be assessed on an annual basis. After due assessment, in appropriate cases, if allowed, the security level should be lowered to reduce the costs of data protection and make data access easier.

9.5 RESPONSIBILITIES UNDER DATA SECURITY MANAGEMENT

The responsibilities of data-related personnel are listed as below, solely intended as an example. The experiences can differ across countries:

a. Owner: the owner has the ownership of the data, the right to manage it and to categorize and grade it, and is the one responsible for the management and maintenance of the data asset.

b. Manager: the manager is authorized to manage relevant data and is in charge of the daily data maintenance and management.

c. Visitor: visitors are allowed to access data within the authorized range and access right limits, and should ensure the confidentiality, integrity and usability of accessed data.

9.6 SECURITY REGULATIONS ON DATA INTEGRITY

Data integrity should comply with the regulations listed below, solely intended as an example. The experiences can differ across countries:

a. The integrity of data management and the technical measure chosen, and their coverage, needs to be ensured.

b. System administration data, including network equipment operation system, host computer operation system, database management systems and application systems, should be detectable. The integrity of information and important business data during transfer should be checked; when there is error, necessary recovery measures can be adopted.

c. Operations, including user access, management and deletion of data, should be fully recorded for audit.

d. For data transferred through non-secure networks, integrity checks should be conducted.

e. A comprehensive access control strategy should be established, which supports the principle of optimizing access rights and limitations.

9.7 SECURITY REQUIREMENTS RELATING TO DATA CONFIDENTIALITY

Security requirements relating to data confidentiality are intended to ensure the secure transfer, application and management of important business information on the business platform, and to make sure such information can be used safely, easily and transparently. Business platforms should use encryption and other security methods to strengthen data confidentiality:

a. Encryption methods should be adopted to ensure confidentiality during the transfer of important business information.

b. Encryption methods should be adopted to ensure confidentiality for important business information during storage.

c. Encryption mainly includes password security and cryptographic key security.

9.8 DATA BACKUP AND RECOVERY

DATA BACKUP REQUIREMENTS:

a. Backup requirements

Media for data backup should be reliable and robust. Information including data resources, backup data and recovery steps should be written on the backup media. The media should be placed in a safe environment.

Under normal circumstances, backup should be carried out periodically (e.g. daily, fortnightly or monthly) for configuration of the server information and network security equipment. Before changing the configuration, or carrying out system upgrades, software patch installation, etc., a backup should also be carried out. Network equipment configuration files should be backed up before version upgrades and configuration changes.

Operation and maintenance personnel should carry out incremental backups of core business data, for example on a daily basis, and backup of all data on weekly basis.

When significant changes are made to the business system, a complete backup should be conducted on core business data.

b. Backup execution and record

The execution of backups should be planned and recorded in detail, including the subject, time, strategy, route and media (type) of the backup.

Backup recovery management requirements may include the following, as examples:

a. Operation and maintenance personnel should plan for the backup data to be tested, £based on the actual needs of different business systems.

b. For general malfunctions, such as those caused by equipment breakdown and operating errors, the backup data needs to be recovered on part of the equipment. Operation and maintenance personnel will need to follow the procedure for handling abnormal incidents and recover the impacted data.

c. Checks and tests on backup media and backup information should be conducted regularly to ensure that they remain useable and effective; it should also be ensured that the system can be recovered in the shortest possible time.

d. Retention periods of key business information and other documents need to be defined.

e. The recovery system should be checked and tested regularly to make sure the operation will be completed within the time set in the recovery operation programme.

f. In the recovery strategy, the backup frequency (e.G. Daily or weekly, incremental or overall) should be decided based on the significance of data and the frequency of introduction of new data.

CHAPTER 10

WCO ONLINE QUESTIONNAIRE 2023: MEMBERS’ PRACTICES FOR SSD APPLICATION ANALYSIS AND FINDINGS

Autec
XCB-0927
Barcelona
Servicio Nacional de Aduana del Ecuador

10

During its 28th Meeting, the SAFE Working Group (SWG) discussed the Study Report on SSDs and decided to continue to explore best practices and innovations in this area, with input from both Customs and the Private Sector. To this end, in January 2023, a Mini-Group on SSDs was re-established among interested delegates of the SWG. The Mini-Group held its first meeting on 8 February 2023 and discussed the constraints raised during various SWG meetings. As a result, the Mini-Group has developed a questionnaire to collect new case studies.

THE QUESTIONNAIRE COVERED THE FOLLOWING TOPICS:

1. Use of ssds by the responding country, types of operations, characteristics, reusability, mode of transport and type of goods concerned.
2. Process of acquisition and management of ssds, associated costs, responsibility for acquisition and ownership.
3. Benefits and challenges of ssds.
4. Components of ssds and technical, legal and procedural conditions for their use.
5. Types of data collected/stored on ssds, responsibility for recording and storing data, interacting with other stakeholders, complying with the wco data model and accessing data.
6. Responsibility for the suspension and removal of ssds, return procedure for devices used internationally.
7. Considering using smart containers as a replacement for SSDs.

On 21 March 2023, the finalized questionnaire was sent to all WCO Members, and was able to collect 37 responses, 24 of which were positive, indicating that these administrations are indeed using SSDs. WCO Members using SSDs include Angola, Australia, Azerbaijan, Belarus, Belgium, China, Côte d'Ivoire, El Salvador, Guatemala, Hong Kong (China), Indonesia, Maldives, Mauritius, Myanmar, Peru, Russian Federation, Saudi Arabia, South Africa, Tanzania, Thailand, Togo, United States, Uzbekistan and Vietnam.

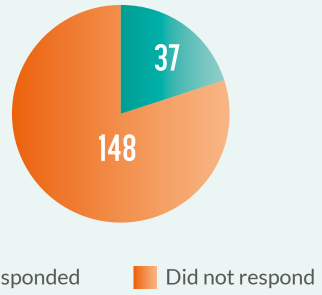
In addition to the responses, Members were asked to share case studies related to the information used in the questionnaire, in order to include them in the updated draft Study Report. This contribution enriched the Report by providing concrete examples of the use of SSDs in different contexts.

ANALYSIS AND FINDINGS:

1. Number of respondents:

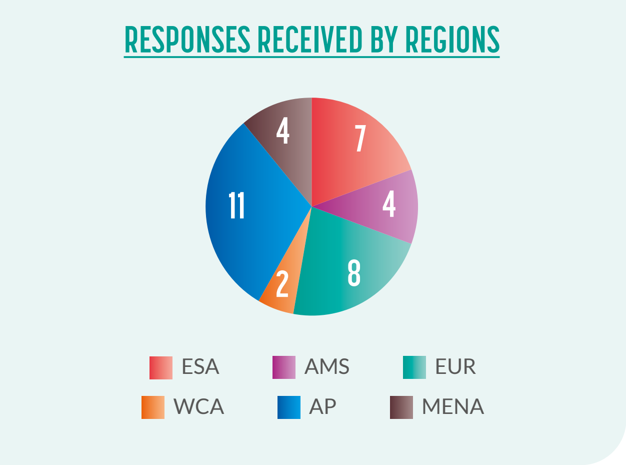
The analysis of the data was based on the responses obtained through a questionnaire circulated to the 185 WCO Members. Of all the Members approached, we received a total of 37 responses, which corresponds to a response rate of 20%.

RESPONDENTS FOR THE SURVEY



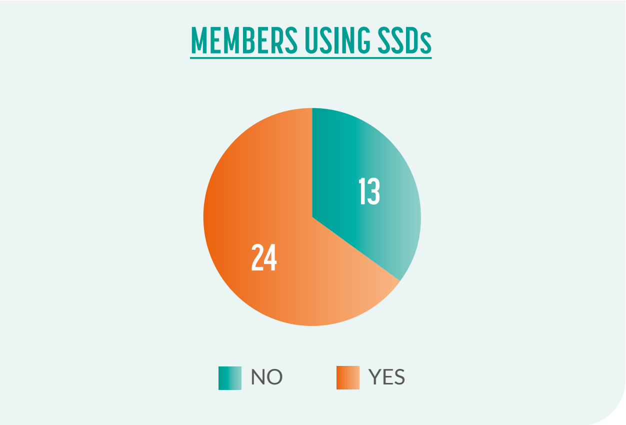
2. Number of respondents by region:

The data analysis also took into account the number of responses received by region, based on the classification of the 185 WCO Members into six distinct regions. Of the 37 responses received, the regional distribution was as follows:


RESPONSES RECEIVED BY REGIONS

3. Number of SSD users:

Of the 37 responses received, a total of 24 responses (approximately 65%) stated that they used SSDs such as electronic seals in their supply chain operations.

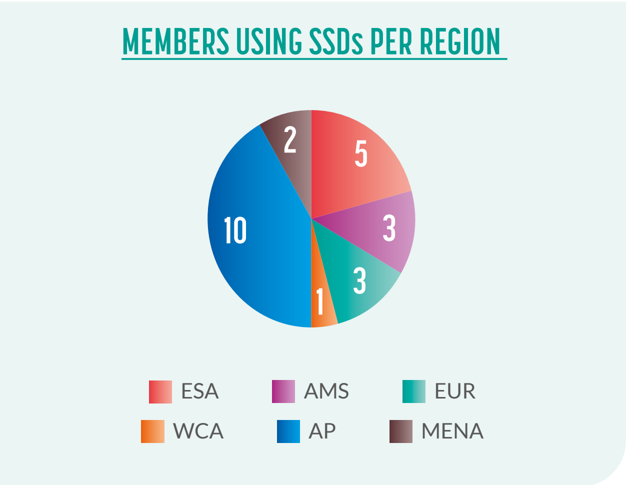

MEMBERS USING SSDs

4. Number of SSD users by region:

The analysis of the data provided by respondents revealed an interesting distribution of SSDs users by region. The North of Africa, Near and Middle East region has two SSD users. Similarly, the West and Central Africa region also has one SSDs user. In contrast, the East and Southern Africa region has a higher uptake, with five SSD users.

In the Americas, the South America, North America, Central America and the Caribbean region reported four SSD users. On the European side, there are three SSD users.

However, the Far East, South and South East Asia, Australasia and the Pacific Islands region stands out, with a significantly higher number of SSD users, at ten users.


MEMBERS USING SSDs PER REGION

5. Number of users of electronic seals:

Among the 24 positive responses indicating the use of SSDs in the supply chain, it is remarkable that electronic seals have been widely adopted by these Members. Electronic seals are confirmed as the primary type of SSDs used in their operations.

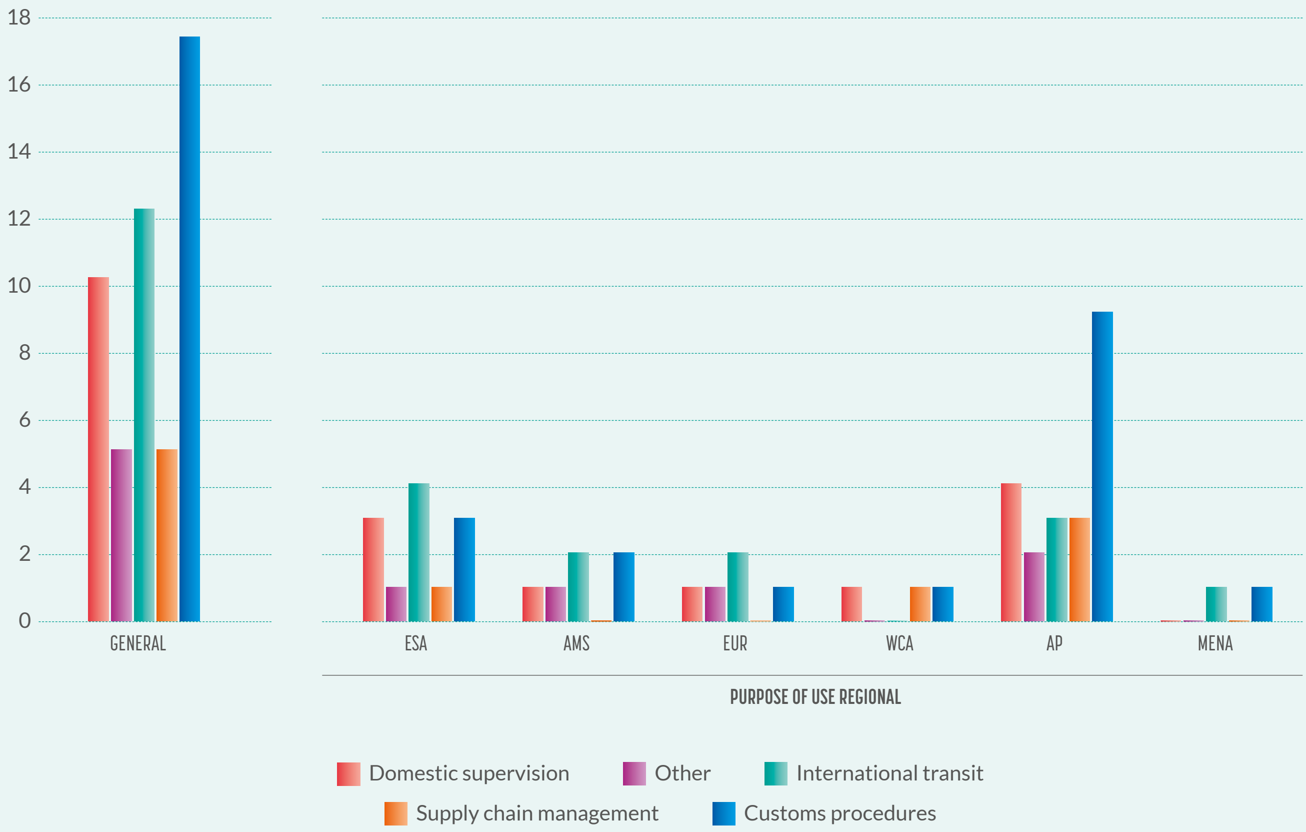
While some of the 24 Members also use other complementary SSDs, it is important to note that electronic seals remain the predominant security technology adopted by these countries.

6. The purpose of using SSDs:

Among the 24 Members who use SSDs, it is interesting to note their use in various operations within their activities. The data collected indicates that Members use SSDs in the following areas: supply chain management (5 responses), Customs procedures (17 responses), domestic supervision (10 responses), international transit (12 responses) and other operations (5 responses).

These results highlight the adaptability and versatility of SSDs in different operational contexts.

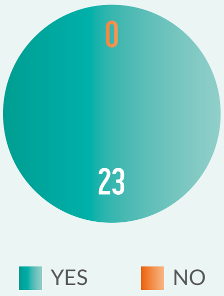
THE PURPOSE OF USING SSDs



7. The reuse of SSDs:

The 24 Members who use SSDs in their operations highlighted a crucial aspect: these devices are reusable.

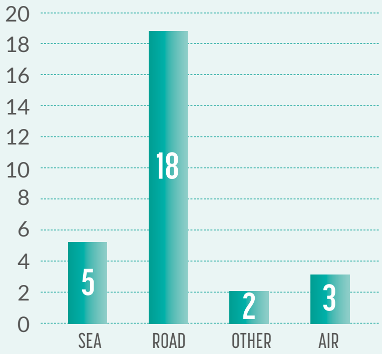
THE REUSABILITY OF SSDs



8. The mode of transport for which SSDs are used:

Members' responses revealed that the use of SSDs extends to different modes of transportation. The data indicate that these devices are adapted and used in a variety of modes of transport, such as air, marine, land and rail.

THE MODE OF TRANSPORT FOR WHICH SSDs ARE USED

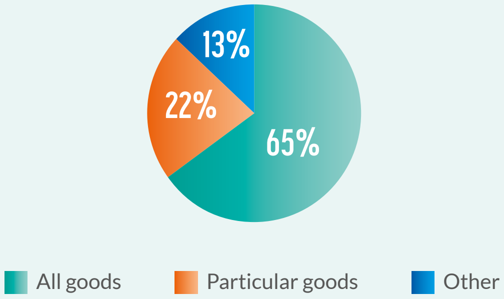


9. The type of goods for which SSDs are used:

The use of SSDs in the supply chain varies by Member and specific situation. In general, they are used to secure all transported goods, ensuring their protection throughout the logistics process.

However, some Members highlighted the use of SSDs for particular goods when specific challenges arise.

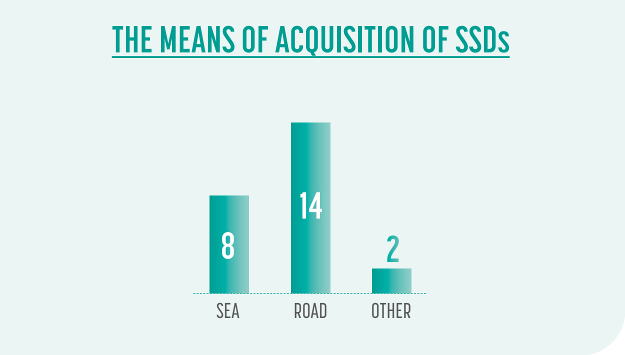
THE TYPE OF GOODS FOR WHICH SSDs ARE USED



10. The means of acquisition of SSDs:

Customs administrations have adopted different approaches to the procurement of SSDs. Most Members have chosen to purchase these devices directly from manufacturers.

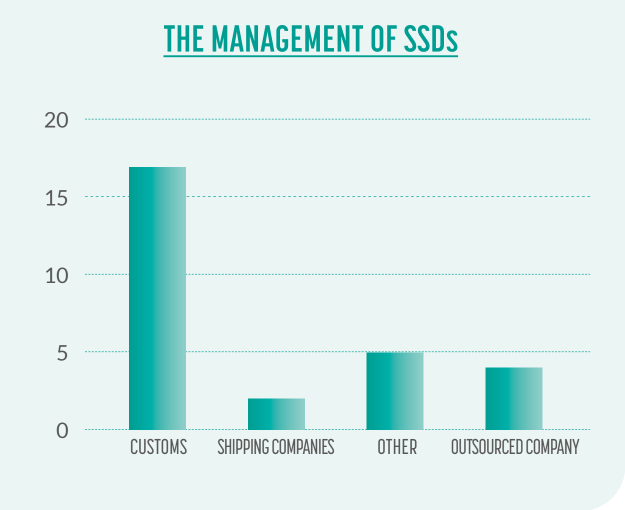
Some Members preferred to use specialized service providers who offer full SSD supervision services in exchange for remuneration, and in rare cases, the leasing option was chosen.



11. SSD management:

Customs administrations are primarily responsible for the management of SSDs.

However, in some cases, management may be shared between Customs, port companies, shipping companies, and logistics service providers, etc.

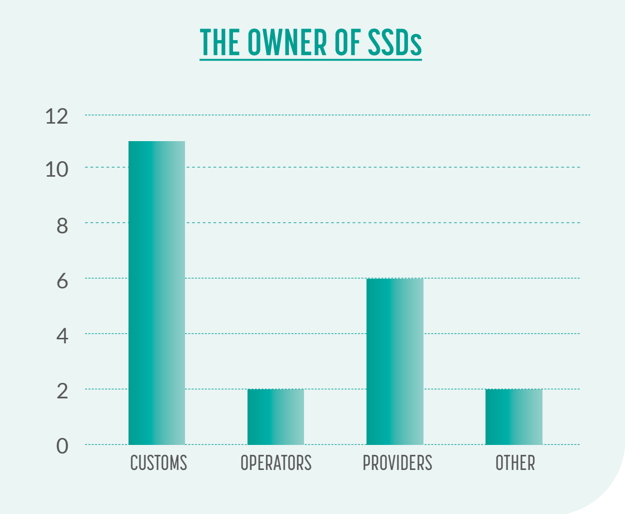


12. The owner of the SSDs:

In most cases, Customs administrations own the SSDs.

However, there are situations where service providers may also own SSDs. This occurs when Customs administrations outsource the management of devices to specialized service providers.

It is important to stress that, even where service providers own SSDs, Customs administrations remain the main managers in these arrangements.



13. Opportunity and benefits/challenges and limitations for SSDs reported via the survey:

OPPORTUNITY AND BENEFITS	DIFFICULTIES AND LIMITATIONS
Real-time monitoring and alerts. Analysis and results of incidents/events. Reduction of physical inspections. Transit control. Intrusion control. Remote unlocking. Effective risk management. Enhanced safety and security against illegal trespassing, robbery, drug trafficking and smuggling. Real-time information on the status of the conveyance/cargo and its integrity that can help Customs and economic operators take timely action and prevent illegal behaviour. Increased supply chain visibility and efficiency and increased productivity of freight movements. Reduced Customs clearance and insurance costs. Goods are controlled from the port of entry to the exit. Ability to track cargo in transit in real time and receive alerts for any route deviations, illegal stops or attempted seal violations during transport. The result: a drastic reduction in the phenomenon of goods returning goods in transit through the Customs territory". Paperwork minimization, fraud prevention, centralized data, online verification of import/export legal aspects with another government agency.	Battery life and variable capacity cost. Very high cost compared to ordinary mechanical seals. Not suitable for non-containerized goods. Difficulty in returning devices during international use. Interoperability problem. Data security. Limited memory capacity. Some places have a limited mobile network, which complicates communication. High maintenance cost. The instability of the GPS signal in some locations could affect the quality of real-time control performed by Customs. The devices and the information they contain are the property of the shipping companies. Some ships do not have the ability to provide electricity, so the device turns off as soon as the battery is discharged. Dependence on network coverage. Signals transmitted from seals to the GSM wave control software system (3G/4G). Sometimes the signal is lost due to displacement in areas without 3G/4G.

14. The technical conditions for the use of SSDs:

It is important to note that the technical requirements for the use of SSDs may vary from Member to Member. These devices have different characteristics depending on their specific use and cost. Some Members may require more advanced technological infrastructures to effectively integrate and manage these devices, while others may have less complex requirements. Technical differences may also arise from device-specific functionalities, such as real-time tracking, compatibility with other systems, or connectivity to Customs platforms.

15. The legal conditions for the use of SSDs:

With regard to legal requirements, Members noted that they generally refer to existing national or regional regulations to govern the use of SSDs.

16. The procedural conditions for the use of SSDs:

It is important to note that the procedures for the use of SSDs may vary depending on each Member's choice of management and the specific purposes for which these devices are used.

17. Data related to the use of SSDs:

a. The person responsible for recording and storing the data:

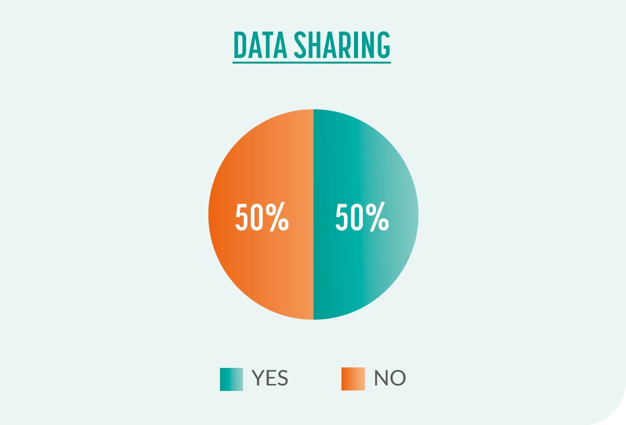
Of the 24 Members, only four reported entrusting the recording and storage of data to their partner vendors. The other Members have chosen to entrust this responsibility exclusively to their own Customs administrations. These administrations themselves collect, record, store and manage data related to SSDs.

b. Exchange of data with stakeholders other than Customs administrations:

Notably, half of the Members surveyed share SSD-related data with other actors in the supply chain.

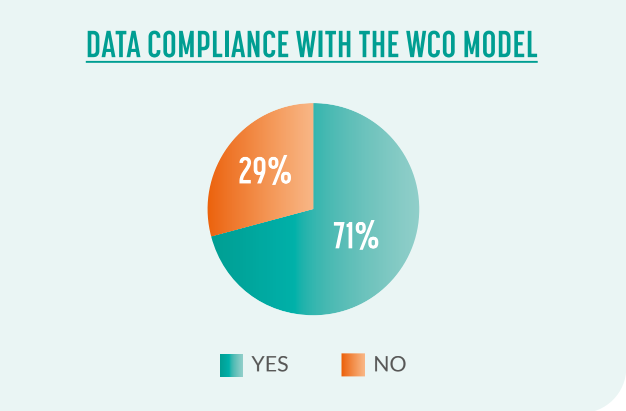
c. Stakeholders who have access to the data:

It is pertinent to note that Members share their SSDs-related data with stakeholders involved in supply chain management.



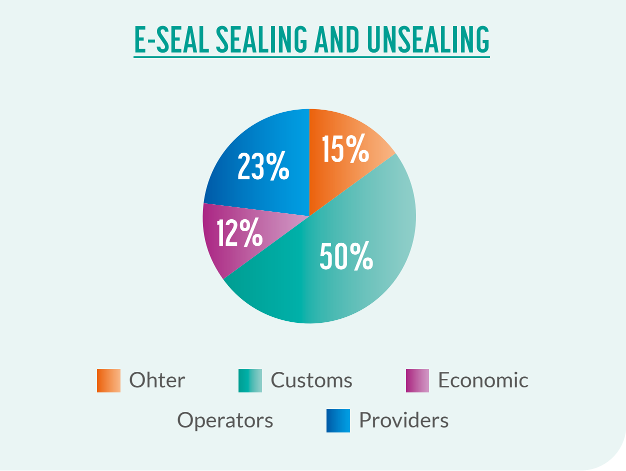
d. Data compliance with the WCO model:

Interestingly, the majority of respondents favour the use of the WCO Data Model for the exchange of SSD-related data.



18. The person responsible for sealing and unsealing:

Members' replies confirm that Customs officers have the primary responsibility for sealing and unsealing these devices.


E-SEAL SEALING AND UNSEALING

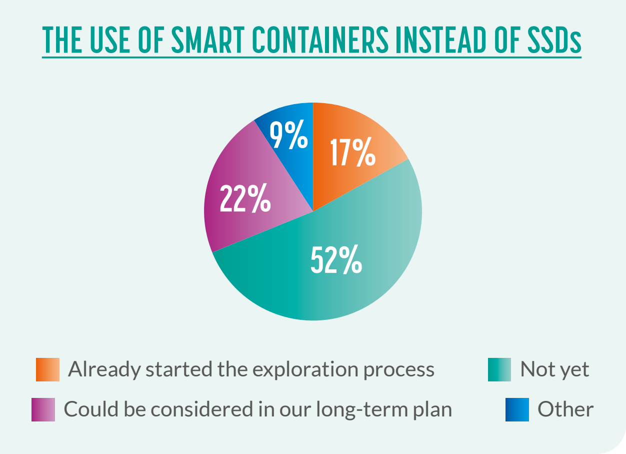
19. The use of smart containers instead of SSDs:

According to the answers obtained, 52% believe that smart containers are not an immediate alternative to electronic sealing. However, these responses suggest that smart containers could eventually become a viable long-term option.

A. Constraints:

1. Constraints relating to definitions:

Common definitions of electronic seals are based mainly on two sources: the Recommendation of the Customs Co-operation Council (CCC) for Customs Procedures Relating to Container Security Devices (CSDs) for Temporary Admission, and ISO 18185.


THE USE OF SMART CONTAINERS INSTEAD OF SSDs

The CSD Recommendation deals with the temporary admission of all security devices, without distinction, while ISO 18185 does not give any specific information on cargo. Therefore, the current definition does not take into account reusable devices, unlike the definition of CSDs in the WCO Recommendation.

ISO 18185 seals offer limited tracking capabilities, only allowing the location and time of recording to be read.

Cost constraints:

The issue of costs was raised several times during discussions on the use of SSDs. The costs associated with the acquisition of these devices, as well as the costs associated with the monitoring platform, are important constraints that must be taken into account.

In summary, cost constraints include the high price of devices, the responsibility for purchasing devices and readers, and the costs associated with the tracking platform. In addition, GPS roaming charges and charging costs must be taken into account, as these devices run on batteries.

2. Requirements constraints:

The constraints raised relate to various requirements that must be known by all parties involved. This includes, first and foremost, the legal and regulatory framework that defines the procedures, rights and obligations of all parties involved in the use of SSDs. In addition, these devices must comply with production characteristics such as battery, resistance to different environments, and ISO and other standards.

3. Data constraints:

Data challenges encompass several aspects, such as the lack of standardized data standards, the diversity of readers offered by different vendors, data management and exchange, data storage and retrieval, the interface between information systems and Customs systems, WCO Data Model compliance, and data security.

Addressing these constraints is of crucial importance for the establishment of an efficient and reliable system. Delegates strive to ensure that data is standardized, secure and reliably accessible.

4. Constraints related to logistics and the procedure for use and the various operational problems:

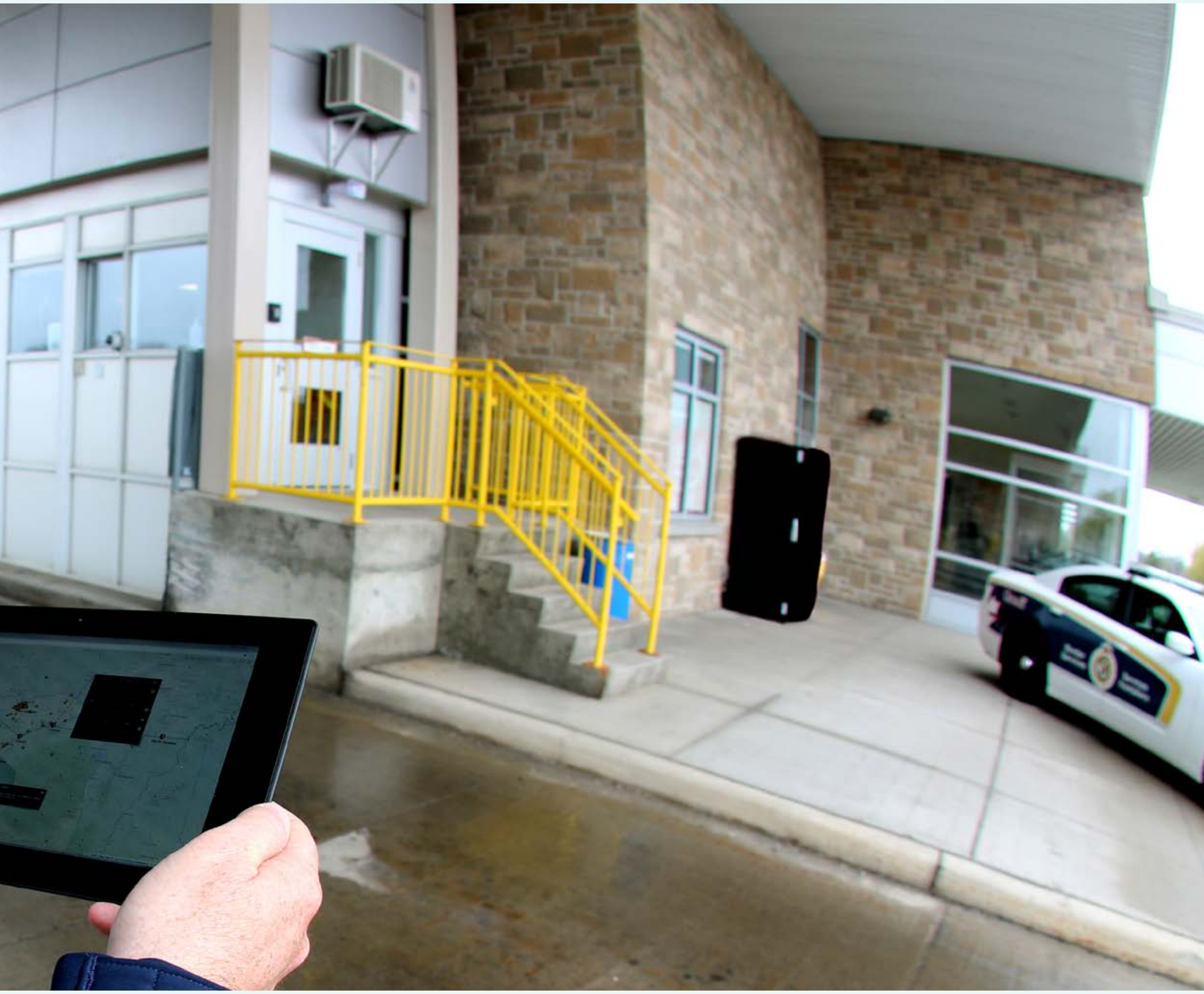
Members expressed concern about the logistical and procedural constraints associated with the use of SSDs. They have questions about the selection of appropriate goods and modes of transport for the application of SSDs, the overall management of these devices,

the return to the starting point in case of international use, the potential consequences of an insufficient number of devices, the person responsible for sealing and unsealing, and the time required for these tasks.

In addition to logistical and procedural concerns, various operational issues were also raised, such as false alarms and cloned devices.

5. Property constraints:

Members of the sector are highly concerned about ownership constraints. Ownership issues include ownership of SSDs, readers, and the platform, as well as ownership of data collected through these means. Members shall endeavour to clarify ownership responsibilities and rights to ensure lawful and equitable use of these technologies. Clarifying these ownership issues is of crucial importance to establishing an effective and reliable system.



CHAPTER 11

CHOOSING THE RIGHT SECURITY TECHNOLOGY

11

The decision to select the most appropriate security technology, whether it is an active device, passive device, semi-active device, or smart container, is a pivotal one. It should be made with careful consideration of the specific security and monitoring requirements inherent to the situation at hand. Each technology has its distinct advantages and weaknesses, and the selection process hinges on a thoughtful evaluation of these factors.

CUSTOMIZING SOLUTIONS TO MATCH UNIQUE NEEDS

The paramount objective when opting for a security technology is to align it precisely with the distinct demands of the situation. This entails a thorough assessment of several critical factors:

a. Security imperatives: the level of security required should be the starting point. For instance, active SSDs offer real-time monitoring and robust security features, while passive SSDs may suffice when covert monitoring takes precedence.

b. Financial considerations: an evaluation of the budget available for security measures is essential. For example, passive SSDs often represent a more cost-effective initial investment, whereas active technologies might require a higher upfront expenditure.

c. Power and maintenance: the power source and maintenance prerequisites should be factored in. Active and semi-active SSDs rely on power sources and may necessitate ongoing maintenance, whereas passive devices are exempt from these requirements.

d. Visibility vs. Covert operations: consider the trade-off between visibility and covert surveillance. Active SSDs, due to their continuous activity, may deter potential threats but can also reveal the presence of security measures.

e. Data necessities: the urgency and scope of data requirements are key. Active SSDs often offer real-time data transmission, while passive devices supply historical data upon inspection.

STRIKING A BALANCE BETWEEN ADVANTAGES AND WEAKNESSES

A comprehensive understanding of the strengths and limitations of each security technology is pivotal for making an informed decision. Active SSDs excel in real-time monitoring, active security features, and visibility, but they entail higher costs and power dependencies. Passive SSDs offer simplicity, covert operation, and minimal maintenance demands, though they lack real-time capabilities.

MAKING A KNOWLEDGEABLE CHOICE

The choice between active, passive, semi-active SSDs, or smart containers should be a discerning one, rooted in the specific security and monitoring needs intrinsic to the situation. Rather than applying a one-size-fits-all approach, organizations and stakeholders should thoughtfully weigh the advantages and weaknesses of each technology. This consideration should encompass factors such as security prerequisites, financial constraints, maintenance concerns, visibility considerations, and data necessities. By aligning the selected technology with the precise demands of the situation, it becomes possible to optimize security measures effectively, while ensuring efficient logistics and the safeguarding of valuable assets.

CHAPTER 12

RECOMMENDATIONS

12

In order to promote the widespread adoption of Smart Security Devices (SSDs) across various countries and regions, the establishment of international technical standards and cooperation frameworks are prerequisites.

1

It might be beneficial to have in place international technical standards on SSDs based on detailed studies and research that could include physical features, contents of stored data, data transfer methods, communication frequency, communication protocol, satellite positioning, data interface, information security, battery life, reliability and other technical specifications of smart security locks, so that they can be applied globally.

2

The WCO should continue further work on the research into the application of SSDs in the international supply chain, and coordinate with other international organizations and stakeholders to develop/update/enhance relevant technical standards.

3

The WCO should continue exploring the application of SSDs along with associated challenges and develop potential solutions in coordination with relevant stakeholders.

4

The WCO should continue exploring the integration of Internet of Things (IoT) devices among different countries and regions, including open-door detection technologies, and should continue further work on the research into the application of smart containers.

WCO OMD

CHAPTER 13

APPENDIX: CASE STUDIES

13.1 APPLICATION OF SMART SECURITY LOCKS ON CHINA RAILWAY EXPRESS BY SLOVAKIA CUSTOMS

With the continuing development of China Railway Express, as one of the major countries along the route Slovakia is witnessing a speedy growth in the transportation volume. To enhance Customs supervision and improve clearance efficiency, the Customs department under the Ministry of Finance of Slovakia took the lead in applying smart security locks on trains travelling through the country. In this project, a transportation supervision system for the Customs department monitoring cross-border cargo was built in Bratislava, allowing real-time supervision on the domestic section of the journey. Integration between smart security locks and a non-intrusive inspection system for railway cargo and vehicles deployed by the Customs department has been achieved. Images produced by non-intrusive inspection machines and related documents can be stored in the mass storage device in smart security locks.

To take things one step further, Slovakia is actively campaigning for a multi-lateral agreement between countries along the China Railway Express route, so that information can be easily exchanged, supervision mutually acknowledged and law enforcement assisted by joint forces. Without compromising the effectiveness of regulation conducted by each country's Customs administration, the application of smart security locks in transit countries will largely improve the clearance speed of cargo carried by China Railway Express.

13.2 APPLICATION OF SMART SECURITY LOCKS FOR REGIONAL TRADE FACILITATION BY THAI CUSTOMS

A container logistics supervision system was implemented by Thai Customs in 2016. In this project, the integrated supervision platform was used in combination with smart security locks. Satellite positioning and tracking, status supervision, and centralized management of cargo information and data on vehicles with imported goods can be carried out during transit at 16 Customs ports across the country. As a result, theft, replacement, smuggling and other illegal activities can be effectively addressed. The level of modernization and management of Customs logistics are being improved accordingly.

To allow data exchange between smart security locks and the supervision platform, a supervision and command centre needed to be built in Bangkok, the capital of Thailand, and supervision stations in each of the 16 Customs ports, with reading and writing devices installed. With a data exchange function and storage of images from non-intrusive inspection machines, containers can be monitored from departure to arrival, with their locations tracked, operations supervised, and data compared, thus improving the level of Customs regulation.

13.3 APPLICATION OF SMART SECURITY LOCKS IN TRANSIT BY HANGZHOU CUSTOMS AND NINGBO CUSTOMS

Small commodities manufactured in Yiwu, Jinghua and a number of other locations in China are popular with international traders. In recent years, cross-border trade in small commodities has maintained a steady momentum. However, as these cities are inland, because of geographical limitations most regulated commodities need to be carried to the port city, Ningbo, by road and shipped across the border.

To further strengthen supervision on transit cargo transportation, and improve clearance efficiency, the local regulation authority, Hangzhou Customs, and port regulation authority, Ningbo Customs, together built a visualized supervision mode covering the two Customs areas. They use smart security locks to connect systems, share data and optimize procedures under the principle of "consistent standards, law enforcement and management." In June 2016, a group of carriers were selected by the two Customs authorities for a trial test on the application of smart security locks. These have been officially implemented in full since December 2017. Since June 2018, the rate of application of smart security locks has remained above 99%.

1. Strengthening supervision: an intelligent logistics supervision platform was built by adapting site structures, providing readers, and adapting other supporting methods, including building infrastructure and carrying out system upgrades. The platform can access three types of information: the communication status, satellite positioning and physical status of smart security locks. Logic parameters and risk thresholds should be set based on the above information, combined with business information and logistic practices, so that regulated commodities can be monitored from lock hanging and sealing, to unsealing and opening, over the entire transportation process. The risk of mixing and replacing goods during transportation is effectively reduced, and the regulatory function is therefore enhanced.
2. Trade facilitation: by optimizing procedures and allowing data exchange, the two Customs authorities aimed to make things easier for companies as much as possible and to use data to the maximum. Companies now only need to make one declaration for commercial transactions involving the two Customs authorities, and the procedure has be made paperless and supports automatic release. Companies are offered more convenience at different stages of clearance, including the submission of declarations, release, and cargo loading. Meanwhile, supported by interaction between handheld readers, fixed readers and smart security locks regarding sealing and unsealing instructions, a 'quick mode' which allows the container to be automatically sealed while moving and automatically unsealed has become a reality. The time spent on sealing has been reduced from 3 minutes on average to around 10 seconds. Fewer human resources are now required and clearance speed has been vastly increased, easing traffic at the port.

In 2018, 267,000 containers used smart security locks on cross-Customs transit; the rate of automatic unsealing exceeded 98%. In the first half of 2019, 181,000 containers used smart security locks, and the automatic unsealing rate remained over 98%.

13.4 SINGLE E-LOCK SCHEME (SELS) – CASE STUDY FROM HONG KONG, CHINA CUSTOMS

To facilitate the movement of transshipment cargoes with simplified Customs clearance process, Hong Kong, China Customs officially launched the Intermodal Transshipment Facilitation Scheme (ITFS) in 2010. Under ITFS, transshipment cargoes will normally be examined once, either at the point of entry or exit. While this saves time by avoiding repeated inspection, Hong Kong, China Customs monitors the transshipment cargoes within the territory via the application of electronic lock (e-lock) and Global Positioning System (GPS) technology together with the provision of advance electronic cargo information.

With a view to further enhancing clearance facilitation, Hong Kong, China Customs and China Customs joined hands to launch the Single E-lock Scheme ('SELS') in 2016 by connecting ITFS with China Customs' Speedy Customs Clearance System, with the use of a single e-lock to build a "green lane" for facilitating logistics flow through seamless clearance service. The two Customs administrations monitor all shipments under SELS based on the principle of "across the boundary with a single e-lock under separate monitoring" to expedite the transshipment process.

Taking the example of air-to-land northbound transshipment, a shipment arriving in Hong Kong, China by air will be loaded onto a cross-boundary vehicle after Customs clearance. The e-lock affixed to the vehicle will be automatically activated and the real-time movement of vehicle will be monitored by GPS technology to ensure the security of the shipment during the journey within the territory. If no irregularities are detected, the e-lock will be automatically deactivated when the shipment arrives at the land boundary control point. The e-lock will be automatically activated again after passing through the entry point on the Mainland China side. Until it reaches the clearance point of Mainland China under the SELS, the e-lock will be deactivated for Customs clearance.

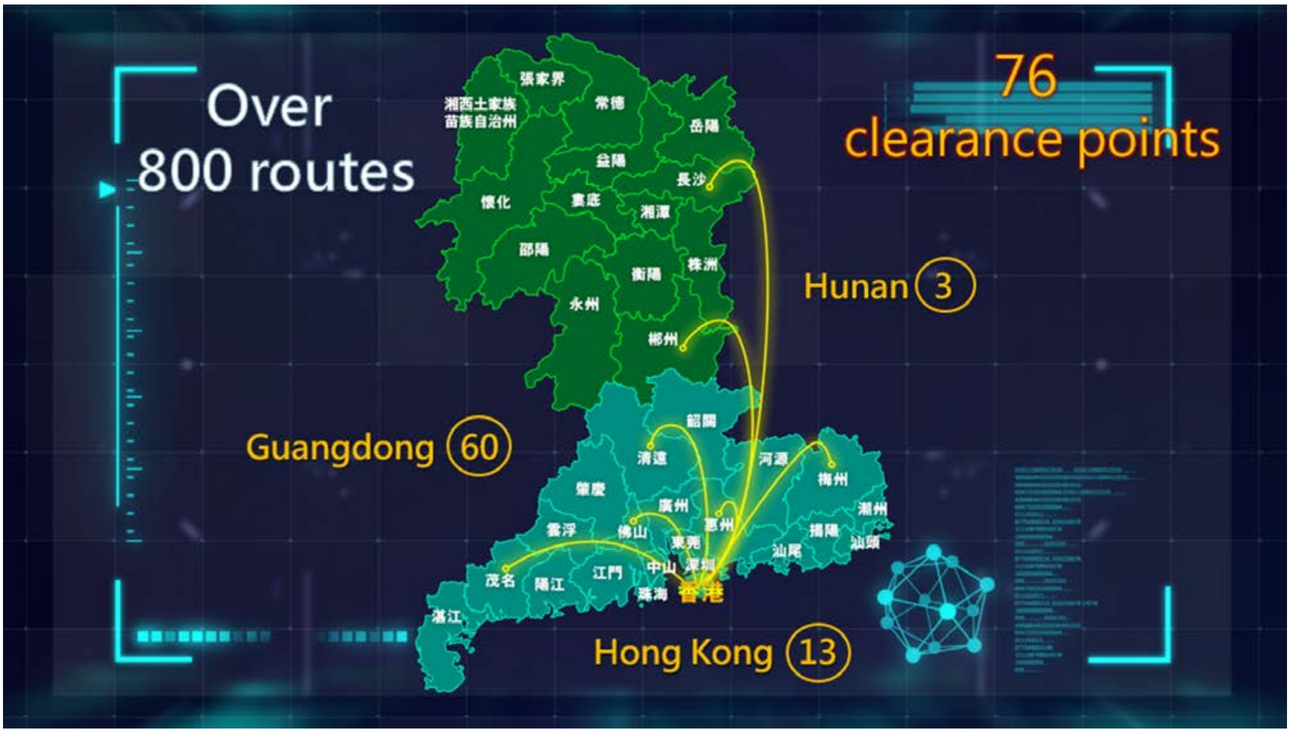
To safeguard against any unauthorized access to the shipment during the entire transshipment process, Hong Kong, China Customs and China Customs will closely monitor the status of the e-lock and track the routing of the vehicle via a real-time monitoring platform.

On 13 June 2023, the coverage of SELS was extended to Hunan Province, which is the second province of Mainland China, after Guangdong Province, to implement the Scheme since 2016. The official launch of clearance points in Hunan has marked a new milestone of SELS in terms of trade facilitation and enhanced security of the cross-boundary supply chain.

The e-lock and GPS equipment share the location of the cross-boundary vehicle and status data with the monitoring platform. If any irregularities are detected, alerts will be triggered, and the transhipment cargoes will be selected for examination.

The Hunan-Guangdong-Hong Kong, China Single E-lock Scheme was officially launched on 13 June 2023, with the first transportation truck departing from Changsha, Hunan.

The first batch of transshipment postal items was successfully delivered to the Hong Kong, China International Airport Air Mail Centre from Changsha, Hunan the next day. The image shows Hong Kong, China Customs officers checking the status of the e-lock that was applied to the batch of transshipment postal items.



The Single E-lock Scheme has been extended to cover 63 clearance points in Guangdong Province and Hunan Province of Mainland China. Together with the 13 clearance points in Hong Kong, China, the Scheme provides trade with over 800 routes for conveying transshipment cargoes across the boundaries.

13.5 CASE STUDIES USING SMART SECURITY DEVICES (SSDs) WITHIN THE EURASIAN ECONOMIC UNION (EAEU)

The most important development stage in this area within the Eurasian Economic Union (EAEU) is the Agreement on using navigation seals (e-seals) for monitoring traffic in the EAEU signed on 19 April 2022.

The Agreement defines the:

- Cases and procedure for using navigation seals.
- Objects subject to monitoring.

- Tracking of participants.
- Modes of transport in respect of which monitoring will be applied.
- Procedure and conditions for applying forms of customs control and other types of state control in the process of transportation of tracking objects.
- Minimization of inspection (examination) of vehicle cargo containers transported with navigation seals.
- Basis of interaction, including the exchange of information, between regulatory authorities, as well as national operators, which should be determined in each eaeu member state, and will ensure the monitoring of traffic in the interests of regulatory authorities.

Regulation of individual issues related to the Agreement's implementation falls within the competence of the Eurasian Economic Commission (uniform technical requirements for navigation seals, determining the procedure and conditions for applying and removing navigation seals, determining the list of excepted goods for which these seals will not be applied, emergency procedures, as well as some technical and organizational issues).

The Agreement contemplates the phase-in monitoring with due regard to the categories of goods and modes of transport by which they will be transported. This approach will ensure the smooth adaptation of traffic participants and public authorities to new up-to-date working conditions.

The implementation of the Agreement will enable the EAEU to:

- Control the movement of goods and vehicles throughout the eaeu in online mode, ensuring the absolute "transparency" of transportation.
- Simplify and expedite the procedure for delivering goods to the recipient.
- Ensure the creation of a common digital space for transit freight transportation in the eaeu territory.

The Agreement is aimed at minimizing state control measures during the transportation of goods (in transit, export and mutual trade) and ensuring their legal turnover.
The minimization of state control measures will reduce business costs, primarily, the time that carriers are now losing to physical inspections carried out by various regulatory authorities. It will also guarantee a reduction in the turnover of illegal goods, which affects bona fide manufacturers and consumers.

Today's realities testify that this new up-to-date control instrument meets the interests of both public authorities and entities engaged in foreign economic activities. The e-seal is a device that monitors the movement of goods and vehicles in the remote mode. Using this technology makes it possible to monitor the vehicle at a distance of hundreds and thousands of kilometres in online mode and record every illegal action involving goods in a sealed cargo compartment, if they occur.

The transportation of goods using e-seals is monitored by means of a monitoring system. Nowadays, each State has its own system, and these systems can be integrated between the parties. The system for monitoring goods traffic is a specialized technological complex designed to perform the functions of collecting, processing, storing and transmitting data in order to monitor traffic using e-seals.

A specific national operator is responsible for ensuring the system's operation and its integration with other similar systems. This national operator interacts with the relevant government authorities and national operators of other States.

The System uses cloud technologies, which makes it possible to scale the System in terms of its productivity, number of users and the amount of information processed. The technologies used enable multiple users to work together on various devices.

Nowadays, e-seals are used mainly for Customs purposes - to control the movement of goods under Customs control. The Republic of Belarus and the Russian Federation in particular have been monitoring traffic using electronic navigation seals since spring 2020. The systems used for cargo monitoring are roughly the same, but they still have some different functionalities.

In the Republic of Belarus, in particular:

- Interaction with the information system of regulatory authorities.
- Real-time identification and monitoring of vehicle movement.
- Real-time notification of tampering (attempted tampering) with the electronic seal, loss of signal or discharge of the e-seal battery, deviation from the route, etc.
- Recording and storing information about the place and time of the event, and identifying the event category.
- Entering photographs and comments following visual control of the state of the e-seal.
- Registration and management of e-seals (battery charge control, assignment to freight traffic, sending commands to open/close electronic seals).
- Creating and administering applications for placing/removing e-seals.
- Mapping freight routes.
- Linking data sources and events to a scalable map, and displaying freight traffic on the map with the possibility to scale and cluster objects.
- Search by freight traffic, e-seals, carriers, users, etc.
- Differentiation of user rights and access to information according to roles.
- Maintaining and storing a log of events, including those related to e-seals.

Initially, the Republic of Belarus used e-seals to monitor motor freight transportation as part of measures to prevent the import and spread of COVID-19, as an alternative to a Customs escort when establishing various carrier violations within the Customs transit procedure, and/or when setting the route. This type of transportation control has demonstrated its efficiency, and therefore, its scope is gradually expanding. The monitoring system created in the Republic of Belarus has proven to be a reliable and universal tool enabling to control the movement of goods and vehicles in the remote mode. In January 2023, the scope of e-seals was expanded in order to control the transportation of high consequence dangerous goods through the territory of the Republic of Belarus. At present, e-seals have been applied to more than 800,000 shipping operations. The number of e-seals simultaneously monitored by the System is 10,000 vehicles per day.

In the Russian Federation, the system's architecture consists of:

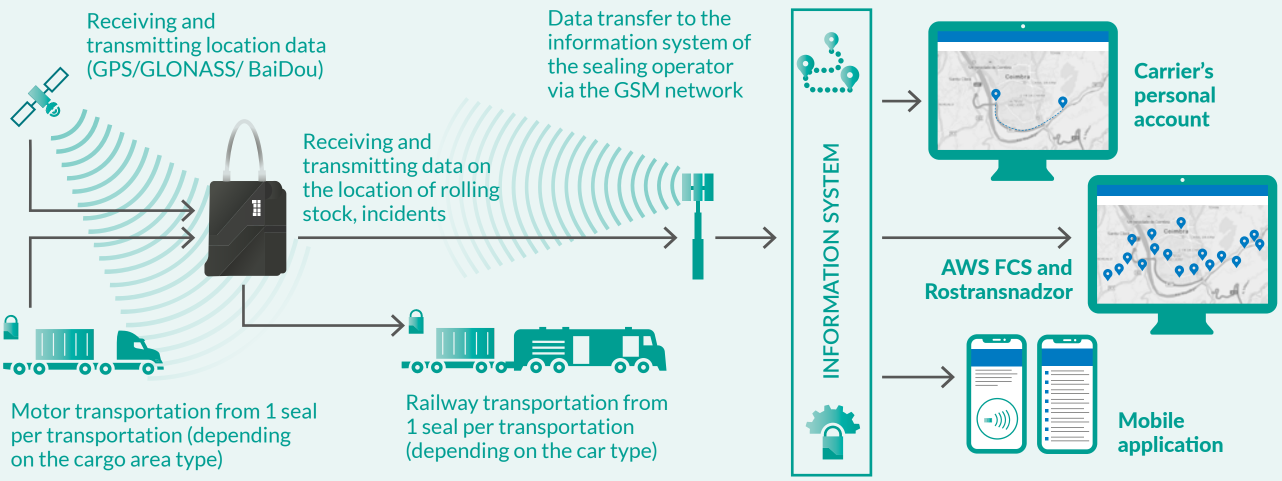
- E-seal - a device enabling monitoring of the coordinates of a sealed object and the status of a reusable sealing element (tampered/ not tampered).
- Monitoring system software - a set of automated workstations supervising the work of all participants in the transportation control process (consignors, freight carriers, freight forwarders and representatives of regulatory authorities who are granted access to the system).
- Data processing centre - a server platform ensuring smooth functioning of the monitoring system.

- External integration module - a standardized interface for data exchange between the monitoring system and external systems of regulatory authorities, freight carriers and commercial customers.
- Specialized mobile device for reading data from the navigation seal and activating/deactivating the device.

As a result, the System provides the following basic functionality:

- Access by regulatory authorities to complete information about the freight traffic and monitoring data of applied navigation seals.
- Carrier's access to data on the location and safety of the cargo.
- Technical monitoring of the e-seal, including the remaining battery power.
- Collection of data on the navigation seal location.
- Ability to remotely control the device in real time.
- Identification of emergency situations requiring a prompt response (tampering with the e-seal, deviation from the route, lack of communication for more than 4 hours).

SCHEME:


Receiving and transmitting location data (GPS/GLONASS/ BaiDou)
Data transfer to the information system of the sealing operator via the GSM network
Receiving and transmitting data on the location of rolling stock, incidents
INFORMATION SYSTEM
Carrier's personal account
AWS FCS and Rostransnadzor
Mobile application
Motor transportation from 1 seal per transportation (depending on the cargo area type)
Railway transportation from 1 seal per transportation (depending on the car type)

The e-seals being used are designed as a fully autonomous device that can operate in a temperature range from -40 to +70 degrees for up to 45 days. The long operating time covers any transit routes through the territory of Russia and neighbouring countries, completely eliminating the seal's dependence on the on-board electric system of the vehicle/rail car. While in operation, the navigation seal ensures registration and regular transmission of the following information to the monitoring system:

- Unauthorized unlocking of navigation seals.
- E-seal malfunction.
- Cutting of the e-seal cable.
- Destruction of the e-seal body.
- Low battery.
- Failure to communicate in the required time (4 hours by default).

Nowadays, the Russian Federation is successfully using e-seals to control the movement of certain categories of goods (especially high-risk goods).

13.6 SMART SECURITY DEVICES IN GLOBAL LOGISTICS: A CASE STUDY ON THE GLOBAL EXPRESS ASSOCIATION'S IMPLEMENTATION AND MANAGEMENT OF SSDs

The Global Express Association (GEA) uses SSDs for supply chain management, domestic supervision, and international transit. As a freight forwarder, broker, and airline, the organization and partner networks leverage the use of SSDs for custodial control with location services, and environmental control with onboard sensors, including but not limited to: light as part of security and photosensitive control of product, temperature at multiple tiers to meet current pharmaceutical and healthcare requirements in transport, shock for potential jarring and damage in transit, and humidity as part of perishable controls. Other sensors are in place to manage regulated control, such as airplane mode and orientation controls in shipping.

TYPES OF SSDs USED BY GEA

GEA uses several types of SSDs, including Model M4, Model ID2, Model ID3, Model ULD Node, and Model ID2S. These devices are reusable and used for all types of goods. They can be used for road, sea, air, and other modes of transport.

BUSINESS MODEL

GEA currently leverages smart containers as part of its freight forwarding products and services, but also as part of its temperature control and air expedited transportation services, domestically within the United States and internationally as part of the organization's network of service.

TECHNICAL AND LEGAL REQUIREMENTS

The SSDs used by GEA, such as the Cellular Radio Devices (Mobile Platform) – M4/ULD and Node Devices (BLE Beacon – Organization Access Point Systems), have technical requirements such as GSM, GPS/A-GPS, BLE, and WiFi communication, and are rechargeable for reusable technology. They also have legal requirements such as FCC, CE, IC, RED, and Local Regional Telecommunication, Ministry of Transport and Customs Allowance, Global Civil Aviation Allowances.

DATA MANAGEMENT

The data from these devices is managed by the owning company. The data is compliant with the WCO Data Model.

DEVICE PLACEMENT AND REMOVAL

Mobile device technology can be placed by the subscription customer as part of the transportation service. All other devices are placed by company personnel governed by employee training and SOP materials for handling and inventory control.

DEVICE COSTS AND OWNERSHIP

All devices and technology provided as part of asset control or the transportation service are wholly owned by the company and move cross-border in a monitoring or active mode. The costs of the devices range from USD3 to USD116.

OPPORTUNITIES AND CHALLENGE

The use of SSDs provides opportunities for better tracking of shipments in cross-border movements, domestic supervision, operational improvements, international transit controls through compliance programmes, and location services. However, the technology is not universally considered a part of the container or an accessory to the shipment, which leads to no globally harmonized control for these moving in cross-border, transit, or return scenarios. This exposes the consumer, transporter, and shipper to additional taxation and duties in these transactions as well as related complexities in capturing these devices on Customs documents.

THE EXAMPLE OF FEDEX

SenseAware is a value-added service which enables shippers to monitor the location of their shipments in near real-time, using GPS technology and environmental conditions such as:

- Temperature.
- Humidity.
- Barometric pressure.
- Exposure to shock (up to 16g).
- Exposure to light.

OVERVIEW	ASSIGNED HS CODE	EXPORT CONTROL REQUIREMENT
Australia	8517.62.0090	No export control required under current DGSL – Defence Trade Controls Act 2012
All EU Member States	First entry: 8526.91.2020 Subsequent entries per BTI ruling: 9027.80.80	No export control required under Regulation EC No 428/2009 amending Regulation EC No 388/2012
Canada	First entry: 8526.91.0020 Subsequent entries - 9814.00.0000	No export control required under current TIE – Groups 1 and 2 – Wassenaur Arrangement 2010
Hong Kong	8526.91.00	No export control required under CAP60G-HSKAR (Sched:1-3)/ TRA CR 436/1015/35
Malaysia	8526.91.000	No export control required under STA 2010-MTI
Puerto Rico	First time through: 8526.91.0040 IIT Return: 9803.00.50	Devices are exempt from Electronic Export Information (EEI) requirements per Foreign Trade Regulations (FTR) classification of EEI 30.37(a) - under 22CFR 120.7 and 15 CFR 730/740
Singapore	8526.91.90	No export control required under Strategic Goods (Control) Act (SGCA)- 2003/SGCL2007
Taiwan	8526.91.00	No export control required under Chapter 3, Article 15, SHTC/2012
United States	First time through: 8526.91.0040 IIT return: 9803.00.50	Devices are exempt from EEI requirements per FTR classification of EEI 30.37(a) - under 22CFR 120.7 and 15 CFR 730/740

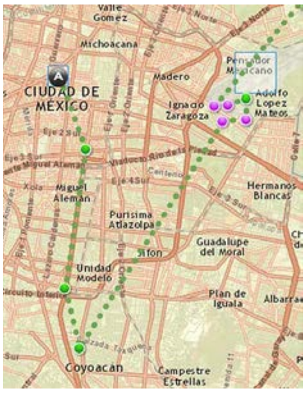
*All shipments with a device monitoring the commodity will have a special instruction or declaration included on the Commercial Invoice/Pro-Forma Invoice: PKG CONTAINS MONITORING DEVICE – FOR FEDEX USE ONLY – NOT FOR SALE.

SenseAware devices are provided to customers as part of the service under contract, for use in approved countries and with approved transporters. The devices are recognized in many countries as accessories to the packaging or container, and even as Instruments of International Trade or Traffic when monitoring commodities. All devices are fully owned by FedEx and are subject to duties and taxes as part of fulfilment routines to international contract customers. FedEx retains all fulfilment documentation as a record of import for subsequent use routines. SenseAware customers are provided with a clearance reference within the application and in training for use as part of fulfilment routines. The chart below references the global clearance routines for international SenseAware shipments.

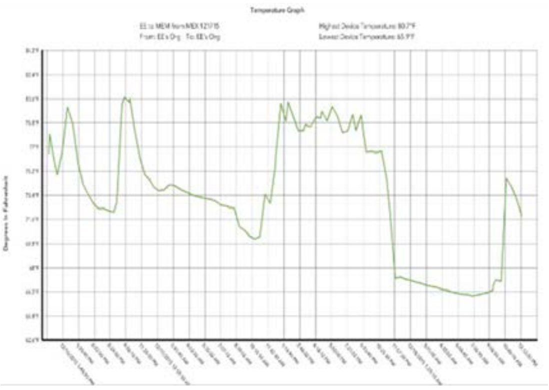
Under the contractual arrangement which governs the SenseAware service, data concerning the location of each shipment, as well as the other metrics monitored, is owned by the shipper which has contracted for, and is paying for, the service. FedEx has access to the data for the sole purpose of providing the service to the customer pursuant to the contract, and FedEx is legally impeded from disclosing the data to any third party. The images below reference the mapping and location data provided to the customer through the web application.

DEVICE MONITORING COMMODITY	DEVICE NOT MONITORING COMMODITY
Device is considered part of the packaging	Device is declared but enters under duty free HS Code
Device is considered an accessory to the packaging Device ID referenced on all entries	Device is declared but enters under duty free HS Code
Device is declared for all entries when monitoring commodity. First entry subject to duty and tax. All subsequent entries are de-clared against as-signed code and duty free	Device is declared for all entries when moving by itself. First entry subject to duty and tax. All subsequent entries are declared against assigned code and duty free
Device is declared but enters under duty free HS Code	Device is declared but enters under duty free HS Code
Device is declared but enters under duty free HS Code Device is considered an accessory to the packaging. Device ID referenced on all entries	Device is declared but enters under duty free HS Code
Device can be considered an Instrument of International Traffic (IIT) under U.S. Customs and Border Protection (CBP) Ruling, or are declared and enter under duty free HS Code (8526.91.0040)	Device is considered an IIT-return under 9803.00.50 or declared under duty free HS Code (8526.91.0040)
Device is declared but enters under duty free HS Code	Device is declared but enters under duty free HS Code
Device is declared but enters under duty free HS Code	Device is declared but enters under duty free HS Code
Device can be considered an IIT under CBP Ruling, or are declared and enter under duty free HS Code (8526.91.0040)	Device is considered an IIT-return under 9803.00.50 or declared under duty free HS Code (8526.91.0040)

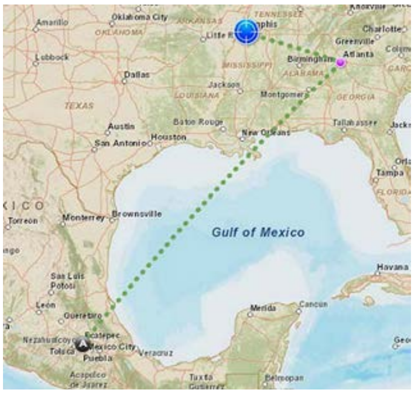
**All shipments containing more than two devices will indicate the proper Lithium Battery declaration on the waybill: "Lithium Batteries in Compliance with UN 3481 Section 2 P.I. 967"



Overall Flight Mapping



Intra-City Mapping



Temperature Graphing

TECHNOLOGY SUPPLIER DECLARATION OF CONFORMITY

Supplier name	FedEx Service, Inc.		
Supplier address	3850 Hacks Cross Rd, Memphis, TN 38125, USA		
Declares under our distribution responsibility of product	SenseAware^{SM}, a FedEx innovation | SenseAware, powered by FedEx		
Device (Devices) market release name	SenseAware^{SM}		
Device (Devices) part name/model	ILC3000 – SenseAware 3000	PT300D – SenseAware PT300D	SenseAware ID Node
Device images			

RADIO TELEPHONE TERMINAL EQUIPMENT EXEMPTED FROM TYPE APPROVAL

NO.	NAME OF MANUFACTURER	NAME OF MODEL	DETAILS CONCERNING THE OPERATION OF EQUIPMENT						
			TECHNOLOGY			FREQUENCY SCOPE (MHZ)			
			GSM	UMTS	BLE	850[4]	900	1800	2100[4]
1.	Moog Inc.	ILC3000[2]	●	●		UBlox – U2 Series GSM 850 MHz	UBlox – U2 Series GSM 900 MHz	UBlox – U2 Series GSM 1800 MHz	UBlox – U2 Series GSM 1900 MHz
2.	Sendum Wireless	PT300D[3]	●	●		RX: 869-885 MHz TX: 824-849 MHz	RX: 925-960 MHz TX: 880-915 MHz	RX: 1930-1990 MHz TX: 1850-1910 MHz	RX: 2110-2170 MHz TX: 1920-1980 MHz
3.	Federal Express	SA-ID2			●	NA	NA	NA	NA

[1] Model ILC2000 is registered for market globally as SenseAware 2000
[2] Model ILC3000 is registered for market globally as SenseAware 3000
[3] Model SA-ID2 is registered for market globally as SenseAware ID
[4] North and South America Frequencies Only – Not Applicable for Israel Telecom

UMTS/GSM Specification – ILC3000

MODEL	TECHNOLOGY		FREQ./BANDS					INTERFACES	FUNCTIONS
	HSUPA (Mb/s)	HSDPA (Mb/s)	850	900	1800	2100	GPRS/ Edge Quad Band	UART, SPI, USB, DCC (Channel 1)	Network/ Antennae Supervision,
U-Blox LISA –U200	5.76	7.2	●	●	●	●	●	GPIO (CH 14)	Jamming Detection, TCP/UDP

6-band W-CDMA (UMTS) and quad-band GPRS/EDGE, LISA-U2 modules are suited for networks worldwide. Features include data-rates of up to 21.1 Mb/s (downlink)

Frequency/Band Specification – PT300D

BAND DESCRIPTION	FREQUENCY	FREQUENCY	FREQUENCY	FREQUENCY
GSM/GPRS/EDGE	850	900	1800	1900
UMTS/HSPA+	800/850 (Band B5-6)	900 (Band 8)	1900 (Band 2)	2100 (B1)
CDMA (1x, EVDO)	800 (BC0/BC10)		1900 (BC1)	

BLE Certification and Specification – SA-ID2

Unintentional Radiators | Specific Absorption Rate (SAR) Compliance (CE/FCC/ISED/RED/ JP RF)	2.4Ghz – BLE In order to comply with FCC / ISED / RED / Japan RF exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

13.7 DEPLOYMENT OF REMOTE CONTAINER MONITORING TECHNOLOGY DURING UK BORDER INNOVATION PILOTS (ECOSYSTEM OF TRUST INITIATIVE) – CASE STUDY FROM MAERSK

In 2021 the UK government outlined its intent to conduct a number of limited pilot projects with industry in order to assess what supply chain visibility and goods integrity capabilities are currently deployed by traders and intermediaries. This was a way to explore how a Public-Private partnership using existing industry solutions could support the implementation of a new world class border model in line with the UK Border Strategy 2025, approved by UK Parliament in December 2020.

The objective of the pilot was to establish the extent to which these could support a trusted trader approach to border management and what benefits could be realised to both the public and private sectors were such a model to be scaled.

Through their involvement via a pilot consortium, AP Moller Maersk were able to demonstrate the capabilities and value of their proprietary Remote Container Monitoring (RCM) platform. RCM was deployed to provide trader-specific supply chain intelligence which could enrich the data available to border authorities and better inform compliance risk profiling. RCM data was submitted to UK Government Agencies, alongside supply chain stakeholder vetting data and supply chain visibility data, to supervise a Trusted Trade Lane through the Port of Felixstowe.

The RCM platform currently provides Maersk with journey and data log information for visibility of container movements and condition, as well as deviation or alarm signalling where particular metrics exceed expected thresholds. Data transmission is supported by both satellite and cellular connections. Customers of Maersk can further obtain access to data log data and various self-service features via the customer-facing product Captain Peter™, which also offers an API output for pushing the data log information to customer or 3rd party systems for analysis.

Specifically, for containers to which said technology was affixed and which were within scope for the pilot, information relating to the consignment's global positioning (GPS), temperature, humidity, power and refrigeration status, as well as cargo probes, was made available to border agencies for analysis.

The pilot did not explore ways in which this type of container integrity data could be integrated with or ingested by relevant government platforms but rather demonstrated the content, quality and consistency of the data. Feedback was positive, with confirmation that additional assurance was provided in excess of that delivered under the current state, particularly for consignments subject to sanitary and phytosanitary controls. An exploration of how to leverage RCM technology and trial it further and more substantively is now ongoing.

NOTES

Contact us:
facilitation@wcoomd.org

Visit our website:
wcoomd.org

Photo credits: © Cover: © Iceland Revenue and Customs – P.6, 103: © World Customs Organization – P.11, 97: © General Authority of Customs of the State of Qatar – P.15, 21, 24-25, 37, 45, 59, 68, 75, 83, 101, 105, 119: © Stock.adobe.com – P.19: Directorate General of Customs of El Salvador – P.27: Curaçao Customs – P.39: Zimbabwe Revenue Authority (ZIMRA) – P.41: Thai Customs Department – P.47: Danish Customs Agency – P. 64: Swedish Customs– P. 72-73: National Customs Agency of Mexico (ANAM) – P. 85: National Customs Service of Ecuador (SENAE) – P. 94-95: Canada Border Services Agency (CBSA) – P. 98: General Directorate of Tunisian Customs.

Publication number: FAC 2024-2 – Legal deposit: D/2025/0448/3

World Customs Organization

Rue du Marché 30, B-1210
Brussels, Belgium
facilitation@wcoomd.org

#WCOOMD
wcoomd.org