CHALMERS
UNIVERSITY OF TECHNOLOGY

Investigating potential effects of IA in road freight transportation and port-terminal logistics

Dealing with contemporary and future aspects of information standards, information systems and information security

Master's thesis in Supply chain Management

Abishek Ganesh Prasad
Hari Haraa Prabu Selvaraj

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF SUPPLY AND OPERATIONS MANAGEMENT

CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2025
www.chalmers.se

Investigating potential effects of IA in road freight transportation and port-terminal logistics

Dealing with contemporary and future aspects of information standards, information systems and information security

ABISHEK GANESH PRASAD
HARI HARAA PRABU SELVARAJ

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Technology Management and Economics
Division of Supply and Operations Management
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2025

Investigating potential effects of IA in road freight transportation and port- terminal logistics

Dealing with contemporary and future aspects of information standards, information systems and information security

ABISHEK GANESH PRASAD
HARI HARAA PRABU SELVARAJ

Supervisor: Gunnar Stefánsson, Department of Technology Management and Economics
Examiner: Gunnar Stefánsson, Department of Technology Management and Economics

Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone + 46 (0)31-772 1000

Gothenburg, Sweden 2025

Investigating potential effects of IA in road freight transportation and port- terminal logistics

Dealing with contemporary and future aspects of information standards, information systems and information security

ABISHEK GANESH PRASAD
HARI HARAA PRABU SELVARAJ

Department of Technology Management and Economics
Chalmers University of Technology

Acknowledgement

This Thesis represents the final extended work resulting from a research journey, so we want to thank everyone who has supported us in our study.

Above all, we extend our sincere gratitude to our supervisor, Stefan Jacobsson, for all the support, constructive feedback, and encouragement he imparted to the growth of our work. We thank our examiner, Gunnar Stefansson, who played a big role in improving and strengthening this thesis through his critical evaluation and insightful suggestions.

Our gratitude is extended to all the experts who generously took time from their schedules to share their valuable insight and experiences with us. Their views have contributed greatly to our understanding of Intelligent Access in road freight and port terminal logistics.

Finally, our acknowledgement goes to the Department of Technology Management and Economics at Chalmers University of Technology for resources and an academic atmosphere without which this research would not have been possible.

This thesis represents the result of a cooperative effort, and everyone involved contributing to its accomplishment is profoundly acknowledged.

Abstract

This thesis explores the application of current and future information standards , information systems, and data security standards to enable Intelligent Access (IA) for road freight transport as well as port-terminal logistics. IA ensures that the right vehicle, with the right load, is on the right road at the right time and is a key enabler for efficient, safe, as well as eco-friendly logistics. With increasing freight volumes as well as increasing demands from regulators, demand for holistic digital access solutions for European logistics chains has been evident.

The research encompasses a broad set of technologies and infrastructures, including information standards, for instance, eFTI, eCMR, RFID, and DATEX II; information systems, for instance, Port Community Systems (PCS), Transport Management Systems (TMS), and Truck Appointment Systems (TAS); and data security, for instance, GDPR, Zero Trust Architecture (ZTA), and blockchain-based verification protocols. The research applies a two-scenario analysis approach to contrast current practice (0-1 year) with future innovation (5-10 years), explaining how these tools together facilitate real-time coordination, reduce inefficiencies, as well as increase compliance in multimodal supply chains.

The findings shows that although much of the logistics system continues to be underused and fragmented especially by small and medium hauliers, the emerging digital infrastructures offer the promise of bringing new levels of interoperability, automation, and cybersecurity. The thesis highlights the strategic value of aligned standards and also trusted data-sharing frameworks in releasing IA's potential.

The research theoretically frames IA as a technology integration and governance problem and provides policymakers, infrastructure regulators, and logistics providers with concrete recommendations to drive digital access control. Empirical testing of IA models, cross-border case studies of implementation, and regulation to encourage scale-up and inclusive digitalization of logistics can represent future research directions.

Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
API	Application programming interface
AMS	Amazon Web Service Managed Services
B2G	Business to Government
C-ITS	Cooperative Intelligent Transport systems
CCAM	Cooperative, Connected and Automated Mobility
DATEX	Data Exchange
DSRC	Dedicated Short Range Communication
DTLF	Digital Transport and Logistics Forum
eCMR	Electronic Consignment Note
EDI	Electronic Data Interchange
eFTI	Electronic Freight Transport Information
ERP	Enterprise Resource Planning
FMS	Fleet Management Systems
G2B	Government to Business
GDPR	The general data protection regulation
I2V	Infrastructure to vehicle
IA	Intelligent Access
IoT	Internet of Things
ITS	Intelligent Transport Systems

JWS	Javascript object Notation Web Signature
LOD	Linked Open Data
ML	Machine Learning
MMTIS	MultiModal Travel Information Systems
NAP	National Access Points
NIS	Network and Information Security
NRA	National Road Authorities
OTM	Open Trip Model
PCS	Port Community System
RFID	Radio Frequency Identification
TAS	Truck Appointment System
TMS	Transport Management System
TOS	Terminal Operating
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
W3C	World Wide Web Consortium
ZTA	Zero trust architecture

Table of Contents

1. Introduction

Road freight transport and terminal-port logistics are quickly being transformed digitally to address long-standing problems like congestion, inefficiency, and fragmented data exchange. As freight volumes increase and environmental regulations become more stringent, intelligent access (IA) has emerged as a vital solution leveraging technologies such as automated gate operations, real-time data exchange, and appointment schemes to improve coordination and streamline flows. This chapter entails an introduction to paint the background and scope of this research front with emphasis on how modern information standards, systems, and security platforms permit smart and efficient access at road-port logistics interfaces.

1.1 Background

The port-terminal logistics and road freight transport information revolution is on a rapid pace with increasing freight volumes, stricter environmental regulations, and the need to optimize infrastructure usage.Intelligent Access(IA) entails providing intelligent solutions to such issues by having the right vehicle with the right load on the right road at the right time (CEDR ISAC, 2024; Jacobsson et al., 2020). The transformation is therefore triggered by the development of new digital standards of information, interoperable systems, and cybersecurity frameworks that jointly intend to remove inefficiencies, ensure data transparency, and support logistics regulatory compliance (Heilig & Voß, 2017; Dasaklis et al., 2024).

Modern day logistics operations still face certain problems, which include congestion, long wait times, and lack of coordinated planning between stakeholders. These inefficiencies are largely a result of limited real-time data sharing and fragmentary system integration, especially for the small and medium hauliers (Jacobsson et al., 2018; Bauk, Schmeink, & Colomer, 2018). Resilient and sustainable port terminal and road freight operations are crying for an answer in the form of intelligent systems such as PCS, TAS and TMS to provide dynamic gate management, container tracking, and appointment scheduling (Chountalas et al., 2024; Tijan et al., 2021).

Past studies highlight the necessity of harmonized digital data streams, especially under the scope of the Electronic Freight Transport Information Regulation (eFTI) (EU 2020/1056), which legally ensures the digital exchange of regulatory freight information from 2025 onwards (European Commission, 2020). Likewise, over 30 ratifications of the electronic Consignment Note (or eCMR, as it goes by its catchy short form) are encouraging the ideals of paperless cross-border operations of transport (Hemeleers, 2023). These standards will constitute the very digital infrastructure allowing for future logistics interoperability and hence permit seamless B2G and G2B integration (Ligteringen, 2021).

Then, advanced data architecture solutions such as OTM and DATEX II will be used for real-time decision-making and access coordination by distinguishing between static and dynamic freight information (OTM Developer Portal, 2023: Delgado et al., 2024). NAPs, under mandate from the EU ITS Directive 2010/40/EU, are centralized platforms for harmonizing multimodal transport data across Member States and are core to access planning and digital permit validation (Mylonas et al., 2023; NAPCORE, 2022).

ITS acts on system levels where V2I, I2V, and V2V communication are used in conjunction with AI routing and automation for compliance enforcement toward emission reduction, congestion mitigation, and safety enhancement (Williams, 2008; Dey et al., 2016). These developments are inline

with the broader vision of the European Green Deal and the TEN-T strategies that regard the need for digital and decarbonized freight corridors (Eurostat, 2022; European Commission, 2020).

With increased importance in the diverse digital logistics landscape come security concerns as logistics systems move into open APIs and cloud infrastructures. Cryptographic guarantees for confidentiality, integrity, and availability of sensitive freight data, in data exchange and decision-making support, are needed. Cybersecurity frameworks such as Zero Trust Architecture (ZTA), GDPR, JWS, and AMS are enforced to support the information exchange for secure, decentralized, event-based decision-making that is tamper-proof (Jones, Bradley, & Sakimura, 2015; CEDR ISAC, 2024; Dasaklis et.al., 2024).

This thesis thus investigates the current and proposed impacts of information standards, systems, and security models vis-à-vis the realization of Intelligent Access in road freight and port-terminal logistics with the benefit of the aforementioned technological, regulatory, and organizational developments. In so doing, using findings, normative mandates, and system innovations, the study seeks to provide a strategic roadmap toward advanced real-time coordination, digital trust, and sustainable access management in Europe's evolving logistics landscape.

1.2 Problem Description

In an era of rapid digitalization of the logistics world, the road freight transport and port-terminal logistics interface still exhibit inefficiencies that cannot be overlooked. Ever-increasing truck queues; varying access procedures and restricted sharing of real-time information; fragmented systems that undermine smooth coordination amongst actors such as hauliers, terminal operators, and regulatory authorities all stand as impediments (Jacobsson et al., 2018; Heilig & Voß, 2017). The small and medium-operated logistics sectors are trapped in a dilemma as many a time, they just do not have the money or technical knowledge how to implement such modernized information systems or register themselves with the newly emerging digital regulations (Bauk, Schmeink, & Colomer, 2018). Thus, lack of an agreed upon and secure digital infrastructure leads to operational inefficiencies, higher costs, and provides little help for authorities to monitor real-time compliance.

The rising volume and complexity of multimodal freight flows throw additional strain on these challenges. The more congested and regulated transport corridors become, the more clear the call for IA solutions is the ones that determine which vehicle, of what load, may enter which road or terminal at which time (CEDR ISAC, 2024).There are several problems interchangeably plaguing road freight and port-terminal logistics and intervening application of information standards, systems and security. Considering an information standard perspective, the nonuniformity across digital document formats is responsible for some delays in cross-border alterations, duplication of effort, and manual errors during processing. Fragmented visibility, irregular data structures, and lower capabilities for automation exist and are perhaps worsened by the absence of formal procedures on such data exchange and lesser use of technologies. In information systems, fragmentation between various platforms results in poor interoperability and slow cargo processing, long truck queues, and inefficient yard operations. Most small and medium logistics operators are limited by the lack of capacity to afford and even integrate such systems, thus widening the divide. Regarding information security, as with any increase in digitalization, the increase of digitalization of logistics processes has made the problem of unauthorized data access, tampering of digital documents, and lack of adequate user authentication emerge.The lack of robust cybersecurity frameworks impeding the implementation of IA (Dasaklis et al., 2024; European Commission, 2020). These issues concern a wide range of stakeholders, including road authorities, port operators, logistics providers, and policymakers, all

requiring reliable, secure, standardized access control mechanisms that enhance efficiency, environmental performance, and enforcement of compliance. This thesis attempts to understand how current and emerging digital standards, systems, and security frameworks can be combined to jointly resolve these urgent issues, enabling a logistics access environment that is ready for the future.

Road freight and terminal-port logistics are defined by eight mutually dependent problems that Intelligent Access (IA) aims to address. Firstly, infrastructure is underutilized due to the absence of dynamic, digital access management, which in turn leads to congestion and underutilization of capacity available (CEDR ISAC, 2024). Secondly, quick road degradation is due to unchecked overweight or poorly routed truck movements, as current systems are helpless to implement weight-based legislation (Heilig & Voß, 2017; Jacobsson et al., 2018). Thirdly, logistics activity does not meet EU climate targets, as truck emissions guzzling is not excluded from environmental areas due to a lack of digital emissions monitoring (European Commission, 2020; Eurostat, 2022). Fourth, terminal and road safety is compromised by a lack of real-time compliance enforcement and limited use of vehicle-to-infrastructure communication (Dey et al., 2016; Williams, 2008). Fifth, a digital divide creates uneven access conditions, as small and medium-sized operators are unable to afford or employ access-enabling technologies in most cases, creating compliance gaps (Bauk, Schmeink, & Colomer, 2018; Jacobsson, 2023). Sixth, high-capacity vehicles (HCVs) and abnormal loads are constrained by manual permit systems and poor digital coordination with capacity in infrastructure (CEDR ISAC, 2024; Ligteringen, 2021). Seventh, infrastructure digital preparedness for HCV routing and smart roads is low as a result of non-interoperable and fragmented systems (Heilig & Voß, 2016; Chountalas et al., 2024). Lastly, cross-border freight transportation is obstructed by digital differences in standards and legal differences in recognition across Member States, which are impediments to seamless digital logistics (Hemelelers, 2023; Dasaklis et al., 2024;CEDR ISAC, 2024). These structural issues require collective digital solutions through offering standard data, system interoperability, and secure data architectures

1.3 Purpose and Research Questions

The purpose of this research is to investigate contemporary and future aspects of information standards, information systems and information security to achieve IA for road freight transportation and port-terminal logistics. It is framed by the following research questions:

1. **What information standards, information systems and information security can be applied contemporarily and in the future for intelligent access in road freight transport and port- and terminal logistics?**

2. **How can these contemporary and future planned information standards, information systems and information security affect intelligent access in road freight transport and port- and terminal logistics?**

1.4 Limitations

Nevertheless, this thesis must recognize certain limitations. First of all, it deals with the interface of road freight transport and port terminal logistics within itself and does not cover other transport modes, such as rail, air, or inland waterways, leaving intermodal dynamics beyond the road-port interface unaddressed.

Secondly, the research is limited to only a few comparatively current and emerging information standards that have been currently acknowledged and used within the European and international logistics portfolio. Examples of these standards include the eFTI (electronic Freight Transport Information) regulatory framework for electronic information exchange, the eCMR (electronic consignment note) protocol, and structures associated with freight documentation and compliance. More general or lesser-known standards have not been studied.

Thirdly, in information systems, the analysis is confined to the systems that really deal with the access management between road hauliers and terminal operators. Examples of such systems include Port Community Systems (PCS), Transport Management Systems (TMS), Truck Appointment Systems (TAS), Fleet Management Systems (FMS), and their various applications in Enterprise Resource Planning (ERP) platforms. Other systems, such as rail operations software or customs-specific IT applications, are beyond the scope of this research.

Finally, the scope of information security is also limited and primarily focuses on the potential applicability of the Amazon web service Managed Services (AMS) and Zero Trust Architecture (ZTA). These frameworks are studied for their potential to secure data exchange in intelligent access services. Wider cybersecurity technology beyond the access control levels are not explored in depth.

2. Literature Review

This chapter explores the current knowledge base and recent advances in the field of intelligent and digitalized logistics, with special emphasis on road freight transport and port and terminal logistics. It begins by analyzing Intelligent Access (IA) systems and the role of the Intelligent Surface Access Community (ISAC) in facilitating optimized and sustainable freight flow through digital technology. The chapter continues with a discussion on port and terminal logistics' operational and technology infrastructure, followed by the role of information standards like eFTI, eCMR, RFID, and EDI in secure and efficient data exchange. It then looks at the evolving dynamics of Business-to-Government (B2G) and Government-to-Business (G2B) interactions and how they have evolved through digital platforms. The chapter evaluates all the major information systems such as PCS, TMS, ERP, FMS, TAS, over and above their interfacing with ITS, geofencing systems and security systems. Then, it outlines the emerging issues in data security and the changing trends while emphasizing selected frameworks such as AMS, Zero Trust Architecture, and cybersecurity benchmarks to assure logistics data integrity and confidentiality. This review forms the backdrop for understanding how digitalization is shaping the logistics ecosystem into one with enhanced operational efficiency, regulatory compliance, and sustainability.

2.1 Intelligent Access

The Intelligent Surface Access Community, or ISAC, is a program that has been established to introduce collaboration in the development and deployment of Intelligent Access(IA) to the solution of road freight management. IA objective is “to have the right vehicle with the right load on the right road at the right time” by utilizing digital technologies. This can result in better road safety, optimized traffic, and environmental conditions. The objective of this research is to examine how new digital data standards and information systems, such as the Electronic Freight Transport Information (eFTI), Electronic Consignment Note (e-CMR),Port Community System (PCS),Truck Appointment System (TAS),Transport Management System (TMS),Fleet Management System (FMS) and Enterprise Resource Planning (ERP) can enhance the efficiency and security of intermodal freight transportation in the road freight transport and port and terminal logistics thus achieving IA.

2.1.1 Intelligent Surface Access Community

The ISAC project focuses on the optimal utilization of infrastructure with a view to minimizing the burden of road capacity management on National Road Authorities.. Smarter traffic control and reduced congestion, along with safety on the roads, would be ensured in integrating IA into NRAs' processes. Additionally, the ISAC project has sought to add value to sustainable freight transport through encouragement of the adoption of digital monitoring and access control systems.

ISAC particularly addresses cross-border freight management, with many of the freight movements taking place outside the borders of the country involved. It deals with the cross-coordination requirements of different countries and how this could be taken into account within IA to achieve movement of goods without violating cross-border regulations. This way, ISAC ensures NRAs get an opportunity to improve their supervision and optimize their road freight activities.

Most ISAC research focuses on automation and digitalization. The project explores how IA may be used along with ITS, connected vehicles, and autonomous driving. NRAs can use these technologies to watch access on the road and ensure that freight moves safely and efficiently.

Another big area of research is security and data standards. ISAC explores how digital freight documentation, such as eFTI (Electronic Freight Transport Information) and e-CMR (Electronic Bill of Lading), can make logistics more efficient. These digital standards allow the processing of transport documents to be handled easily and increase the security of sensitive information, such as information classified for military use.

In terms of smart roads and infrastructure management, the project explores how to optimize freight transport through innovations in smart parking, automatic traffic control, and the monitoring of infrastructure. High capacity transport can therefore be managed through these digital tools to ensure usage of roads remains optimal and road safety is promoted.

2.1.2 National Road Authorities(NRA)

Digital transformation in NRAs and logistics industry holds significant prospects to enhance monitoring of roads as well as controlling access. It is through National Road Authorities that the implementation of IA solutions comes into the fold. One of the biggest worries of NRAs is traffic congestion management. IA optimizes freight movement, preventing bottlenecks, and ensuring smooth traffic flow.

Compliance with regulations is another fundamental concern for NRAs. With IA, authorities can more effectively monitor and enforce weight, speed, and environmental regulations. Through the use of integration of digital monitoring devices, they can confirm freight operators are complying with the rules without on-going physical inspections.

ISAC also improves the efficiency of intermodal transportation. Freight moves through several modes of transport, such as road, sea, and rail.IA also supports easy coordination of these transport networks through digital standardization of freight documentation, thereby reducing delays and improving operational efficiency.

ISAC project becomes a reality for having a smart, efficient, and sustainable freight transport system. Cooperation between the road authorities, logistics operators, and innovators in technologies make sure that IA solutions are put to maximum use across various regions.Continuous research and development will make sure that IA would be at the heart of transport policy in the future, including better road safety and optimal utilization of infrastructure. Through digital transformation, NRAs can establish smarter and more sustainable road freight networks for economy and environment alike.

2.2 Port and terminal logistics

In global supply chains, port and terminal logistics become major 'interfaces' due to the specific modalities under which they operate and the connectivities between maritime and inland transport systems (Ligteringen, 2021). Such facilities will serve as a means in the effective movement, transfer, and temporary storage of cargo among the various modes of transport (Ligteringen, 2021). The efficiencies that port logistics offer will thus significantly impact trade efficiency, supply chain reliability and regional economic development (Notteboom, Pallis & Rodrigue, 2022).

The terminal logistics operations comprise three phases of operation: pre-access, the access phase, and the post-access phase (Jacobsson, 2023). Pre-access preparations will include documentation and scheduling (Jacobsson, 2023). The access phase consists of loading and unloading containers and cargo (Jacobsson, 2023). Post-access consists of coordinating delivery, storage, or transportation onward (Jacobsson, 2023). During these phases, insufficient coordination may lead to unnecessary movements, congestion, or the increased turnaround time (Jacobsson, 2023).

Automation technologies have redefined this terminal logistics arena by cutting down on human intervention to achieve higher operation effectiveness (Martín-Soberón et al., 2014). Equipment such as Automated Guided Vehicles and Automated Stacking Cranes standardizes handling procedures and cutting down on labor dependency and having a robustness in safety (Martín-Soberón et al., 2014). These improvements work particularly well with container terminals as the goods and processes are homogeneous (Martín-Soberón et al., 2014).

On the other hand, the adoption of access management systems with automated gate services has resulted in greater efficiency with reduced times of queuing and overall truck turnaround times (Jacobsson & Lantz, 2024). It must be noted here that by such Automated gate services implementation, turnaround time was reduced by 17%, while queuing time was cut down by 38% (Jacobsson & Lantz, 2024). Real-time data sharing among terminal operators, road hauliers, and rail operators through interoperable information systems would also improve coordinated access (Jacobsson, Arnäs & Stefansson, 2020).

Smart Ports or Port 4.0 will probably emerge as one of the new faces of port evolution: port automation, sustainability, and collaboration through digitalization (Heikkilä, Saarni & Saurama, 2022). Today's technologies, such as the Internet of Things, big data, and blockchain, link operations with visibility, traceability, and decision-making in real time (Heilig & Voß, 2016). Yet, despite this promise, many ports are still using outdated systems, such as spreadsheets, highlighting the digital divide in the maritime industry (Heikkilä et al. 2022).

2.3 Road freight transportation

Road freight transport is the backbone of global logistics, moving products both short and long distances with responsiveness, availability, and flexibility. Road freight is used in supply chains to transport products in time for manufacturing, retail, and e-commerce companies. Road freight is much better than rail or sea freight with door-to-door pick-up and delivery, flexible routes, and quick response to market needs (Jacobsson, 2023).

Road freight transport, with all its benefits, is beset by a number of issues, including traffic congestion, fuel prices, carbon emissions, and terminal access inefficiencies. Evidence suggests that long wait times, congestion, and inefficient access management at freight terminals have a significant impact on operational efficiency (Jacobsson & Lantz, 2024). Moreover, environmental concerns have precipitated increasing pressure for low-emission vehicles, alternative fuel, and improved route planning measures (Jacobsson et al., 2020).

The industry is being met with digitalization for improved efficiency, security, and sustainability. Electronic Freight Transport Information (eFTI) and the electronic Consignment Note (eCMR) lower administrative costs by facilitating real-time digital data exchange. Moreover, Intelligent Access (IA) systems facilitate the right vehicle with the right load on the right road at the right time, maximizing freight mobility and minimizing congestion (Jacobsson et al., 2018).

Moreover, telematics, fleet management systems, and automated gate services are improving efficiency by streamlining customs clearance, idle time reduction, and truck turnaround time optimization at terminals. Use of Radio-Frequency Identification (RFID) and Electronic Data Interchange (EDI) also improves real-time monitoring, security, and supply chain transparency further (Jacobsson et al., 2017).

Future road freight transport will be powered by digitalization, automation, and sustainability. Electric and hydrogen trucks cutting carbon, employing AI-based logistics, and other smart infrastructures will be the pillars for efficient, low-cost, and low-carbon freight transport. Breaking regulatory, technology, and security barriers will become the imperative to build a robust, competitive road freight industry (Jacobsson, 2019).

2.4 Information standards in Road Freight Transportation and Port and Terminal Logistics

2.4.1 EDI and RFID as Information Standards

In the current context , Electronic Data Interchange (EDI) and Radio Frequency Identification (RFID) have become core information standards enabling real-time visibility, process optimization, and secure information sharing in road freight and terminal/port logistics. RFID is associated with automatic goods/transport unit tracking through embedded tags and networked sensors. Its basic advantage is in enabling real-time capture at control points such as port gate of entrance or warehouse docks, saving time lost through manual checking or human mistake (Shi, Tao, & Voß, 2011). Concurrently, EDI enables structured information interchange of core documents such as shipping manifests, bills of lading, and customs statements between logistics stakeholders, replacing time-consuming, error-prone manual processing with frictionless flows of communication (Heilig & Voß, 2016). Together, the two standards enable standardization and automation of basic activities such as cargo check-in, clearance, and multimodal handover.

Together, RFID and EDI technology create an integrated logistics environment where cargo status and condition information as well as cargo identification are automatically transmitted and mapped on standard documentation flows. For example, RFID tags on containers can signal position or security status while EDI systems simultaneously receive document flows like eCMR or waybills. Synching minimizes delay times, removes document mismatch discrepancies, and makes each movement of cargo traceable and regulatory compliant. Integrating RFID on EDI processes, as Imburgia (2006) suggests, builds a competitive strength through increased visibility for information as well as lead time and bullwhip effect minimization in the entire process of the supply chain. Implementation barriers currently lie in harmonization of in-place systems, diverging standard take-up between jurisdictions as well as high levels of cybersecurity protection requirements. The infrastructure particularly of developing ports may not be in place to support high-end RFID/EDI interoperability or decryption processes, and modular upgrade of systems in incremental take-up becomes more feasible (Bauk, Schmeink, & Colomer, 2018).

In the future, RFID and EDI transform into more sophisticated, interconnected systems part of larger Internet of Things (IoT) and regulatory standard infrastructures. New-generation RFID tags are more sophisticated through the integration of sensors, GPS functionality, and tamper detection for enabling prediction of cargo routing, geofencing for access control purposes, and exception-based alarms. RFID-enabled systems of the future will communicate with automatic Truck Appointment Systems (TAS) and Terminal Operating Systems (TOS) to implement Intelligent Access (IA) on the basis of pre-defined attributes such as emission category, vehicle mass, or time window of receipt. EDI in the future merges with future regulatory requirements such as the EU's Electronic Freight Transport Information (eFTI) Regulation and the electronic consignment note (eCMR) to offer seamless and borderless paperless logistics. EDI platforms of the future not only transfer documents but also automatically update rules of access and indicators of conformity in real time from real-time RFID inputs (European Commission, 2020).

Apart from all of the above, RFID will be becoming more widely used at the edges of IoT ecosystems to enable decentralized networks of information nodes providing real-time information into centralized decision platforms. One such application is RFID-tagged e-seals which can authenticate container intactness during transit and automatically initiate customs pre-clearance processes if intact, reducing dwell times at border terminals (Shi, Tao, & Voß, 2011). EDI systems in such an environment will act as backbones for Transport Management Systems (TMS) and Freight Management Systems (FMS), from scheduling through billing and reporting on compliances. High-end RFID installations according to Bauk et al. (2018) will also be utilized for worker and goods safety in transitional port environments for traceability, distress signals for emergency purposes, and environmental monitoring. To safeguard against loss of integrity in such environments of being too well-connected, RFID and EDI systems will require strong cryptography, authentication layers and potentially blockchain-audit trails in order to offer trust and against potential tampering.

2.4.2 Open Trip Model

The Open Trip Model (OTM) is an open-source model for exchanging data designed for standardizing and enabling logistics information exchange among transport and logistics stakeholders. Simacan developed it, and it is now supported by Stichting Uniforme Transport Code (SUTC). OTM supports carriers, municipalities, shipping companies, and logistics-active organizations with standardized communication (OpenTripModel.org, n.d.). Its architecture is specifically suited for simulating freight movement's dynamics and handling dynamic relations among actors within the transport chain.
One of the defining features of OTM is differentiation among static and dynamic data. Dynamic objects hold relatively stable items such as consignment numbers, vehicles, and stops, while dynamic data comprises events, actions, and status such as trip status, loading activities, or telematics input that change with time (OTM Developer Portal, 2023). The structured yet dynamic nature allows for real-time logistics visibility that is a requirement for coordination and decision-making.
The flexibility of the model lies in it being adaptive for multiple use cases within logistics, with optional fields, and multiple modeling possibilities. However, for a harmonized functionality within companies and systems, specific OTM profiles were created for provision of structured configurations for specific scenarios (OTM Developer Portal, 2023). This has made real-life deployments feasible, for instance, a case of OTM use by Aventeon for optimizing transport execution data exchange among carriers and shippers, a reality. The use by Aventeon indicated that use of OTM makes integrating IT systems simpler and augments real-time knowledge with logistics processes (Aventeon, 2023).
Most importantly, OTM is well suited for Intelligent Access (IA) of terminal-port and road freight logistics. Through provision of a machine-readable, semantically encoded representation of a data model for trips and associated events, OTM can be leveraged to provide required access conditions like vehicle category, load category, emission category, and time slot authorization to traffic control units or infrastructure authorities. This facilitates intelligent decisions about whether a certain vehicle is or is not authorized to use a section of a road, an urban zone, or terminal area based on digital permit conditions or operational restrictions. Combined with real-time systems such as Truck Appointment Systems (TAS) and Vehicle-to-Infrastructure (V2I) communication systems, OTM can provide the bottom data layer for dynamic, criteria-based regulation of access according to Intelligent Access principles (Aventeon, 2023; OTM Developer Portal, 2023).

In the next five to ten years , Open Trip Model (OTM) will be one of the key facilitators of future logistics' digitalization and next-generation multi-partner collaboration in European freight. As ever more logistics becomes dependent on real-time data exchange, automation and AI-coordinated process control, OTM's formally designed extensible data model makes OTM an attractive infrastructure component for policy-governed control of logistics across varied systems. Future

versions of OTM will also underpin digital transport corridors, autonomous driving platforms, and decentralized trust networks in the development of end-to-end data-driven logistics infrastructure (OTM Developer Portal, 2023; OpenTripModel.org, n.d.).

The semantic expressiveness and machine-machine compatibility of OTM are also ideally geared to support the regulatory-conformant and automated Intelligent Access (IA) operations. OTM will be a base schema for expressing transport intention, emissions credentials, and routing and load type preference pre-checked against digitally defined rules of access in the future's digitalized freight corridors. This will allow infrastructure managers to automatically permit or prohibit access through geofenced lanes, low-emission streets, or dynamically congested infrastructures with no human intervention, a direct facilitator of automation of compliance enforcement (OpenTripModel.org, n.d.). Along with it, OTM will be supplemented with the use of other forthcoming paradigms in the digital space such as the eFTI Regulation on electronic Freight Transport Information, DTLF vision of an EU federated platform, and JSON Web Signatures (JWS) for tamper-evident logging of events. These bridges will make OTM not only a logistics modeling tool but also an auditable log of event-driven transactions and access control decisions for multi-actor systems (OTM Developer Portal, 2023). When national and EU-level logistics policies become more developed, OTM can be anticipated to be used as a standardization model for transport declarations, emissions disclosures, and infrastructure usage triggered by smart contracts for transparency, efficiency, and sustainability.

2.4.3 Electronic Freight Transport Information(eFTI)

In the current logistics scene, roll-out planning of the Electronic Freight Transport Information (eFTI) Regulation (EU 2020/1056) continues with infrastructure development and outreach to various stakeholders being the most prevalent activities in the majority of Member States. Although the regulation became effective in August of 2020, its full roll-out is not yet compulsory. Institutions such as Traficom in Finland and logistics coordination institutions across the EU are currently busy designing technical interfaces such as eFTI Gates and Authority Access Points as foundational building blocks for economic operator-competent authority safe data exchange (Nykänen et al., 2024). On the other hand, initiatives such as the CINEA-funded eFTI4EU project for nine Member States are establishing the basis for an interoperable open-source eFTI platform environment for cross-border freight data harmonization (Nykänen et al., 2024).

Despite technological development, readiness and awareness among logistics companies are low. Interviews in the Finnish context point out that while most of the firms have an optimistic attitude towards eFTI, they have limited detailed knowledge about its impact and technical details. Challenges in terms of decentralized IT infrastructure, knowledge gaps in the online arena, and cybersecurity issues mark the present context (Dasaklis et al., 2024). In port and terminal logistics where parties like customs authorities, terminal operators, and shipping lines come into play, eFTI has the ability to reduce the volume of paper documents, expedite cargo checking, and enable real-time compliances. These benefits are not achieved to optimum levels due to the lack of harmonized IT infrastructure in systems like Port Community Systems (PCS) and Transport Management Systems (TMS) (Chountalas et al., 2024).

From 2027 onwards, eFTI will be an obligatory digital standard for the EU Member States' authorities who will be obliged to receive freight regulatory information through certified platforms (European Commission, 2025). It's a new way of sharing logistics information between borders and between public and private stakeholders. eFTI architecture will be composed of economic operator hosted certified eFTI platforms, eFTI service providers, and national and authority access points. The

systems will facilitate the seamless sharing of data between business and authority (B2A), regulatory conformity, and operational performance (Chountalas et al., 2024).

In future port and terminal logistics, eFTI will support real-time standardised and secure information exchange. The regulation's pull-model approach for the data access model—that of being pulled from where it is stored, rather than being given—will enhance control and visibility of the information (Nykänen et al., 2024). Harmonised semantics and standardised interfaces on the basis of standardisations like UN/CEFACT and W3C Verifiable Credentials will support eFTI in offering multi-modal integration to enable interoperability between maritime, road, and rail systems (Hemeleers, 2023). Increased maturity on platforms will have eFTI reducing dwell time for cargo, automation of document verification, and promotion of green logistics through minimising paper transactions. However, success in the future will be in accordance with bringing SMEs digitally on board, harmonization of national laws, and financing stakeholders' training (Dasaklis et al., 2024)

2.4.4 Electronic Consignment Note(eCMR)

The electronic Consignment Note (eCMR) is the corresponding electronic variant of the traditional CMR for road transport in the context of the United Nations CMR Convention. Ratified by over 30 countries, including all of the major EU countries, its application in terminal and port logistics is partial and pilot-led. eCMR is currently implemented in selected cross-border operations and mixed logistics environments, e.g., in the EU-Gate Living Lab 17 project, where coordinated transports of beer and wine between France, Belgium, and Spain were performed using interoperable eCMR and eFTI systems (Hemeleers, 2023).

In actual operations, eCMR allows real-time sharing of documents between shippers, terminals, customs authorities, and carriers. eCMR enhances the integrity of information through time-stamping and secure electronic signatures to preclude loss of documents as well as manipulation (Dasaklis et al., 2024). Integration of eCMR with ERP systems and transportation management systems makes it possible to track consignments automatically and has eased customs verification processes. Most stakeholders are not in favor of abandoning the use of paper due to issues of legal acceptance, incompatibility of infrastructure, as well as prohibitively high transition costs (Chountalas et al., 2024). These issues deter the general application of eCMR in ports where the coordination of multiple stakeholders is required.

In the future decade, eCMR will become standard for EU road freight, particularly as a part of the EU digitalization of logistics to support the EU Green Deal. In alignment with systems like eFTI, PCS, and TOS, eCMR will facilitate fully digital end-to-end processes for all stages from order creation all the way to confirm final delivery. Its formal status will be settled as part of harmonized European transport data space in order to support mutual recognition in all Member States and in all logistics environments (Chountalas et al., 2024).

The future integration of eCMR with eFTI, Transport Management Systems (TMS), and customs clearance systems will introduce high levels of automation in operations. Examples of benefits to be introduced through the integration are real-time updation of consignment status, auto-invoicing, and decongestion of ports through vehicle scheduling optimization. In addition, eCMR will promote environmental sustainability through avoidance of use of paper and dwell time reduction at checkpoints. Utilization of technologies like W3C decentralized identifiers and verifiable credentials will enhance privacy and trust in logistics transactions (Hemeleers, 2023). However, attainment of

these benefits fully depends on harmonized conformity of legislations, economic incentives to SMEs, and large-scale training of logistics employees in digital technologies.

2.4.5 Business-to-Government (B2G) and Government-to-Business (G2B)

B2G (Business-to-Government) is the interaction and exchange between government agencies and private businesses. Generally, the interactions are of the type of the provision of goods, services, or information by private businesses to government agencies. In transport and logistics businesses, B2G interactions are significant in efficient management of the transport infrastructure such as roads, terminals, and ports. Private logistics businesses, for example, provide fleet management systems, transport management systems (TMS), and other software programs to government agencies to enable the movement of goods and services (European Commission, 2020).

On the other hand, G2B interactions encompass government agencies delivering services or information to business firms. Examples of such services include issuing licenses, offering access to public information, and enabling regulatory compliance. In road freight transport, for example, governments offer G2B services like customs clearance systems and truck scheduling programs for terminals and ports. Such services help companies improve their business by ensuring their vehicles are compliant with the government and processed easily at customs (Heilig & Voß, 2016). Both the B2G and G2B relationships critically depend on a good information system and data standards to facilitate facile communication and fruitful data transfer from the private and public sectors.

In contemporary times (0-1 year), application of information standards and digital technologies such as Electronic Freight Transport Information (eFTI) and the Electronic Consignment Note (eCMR) has commenced transforming both B2G and G2B interfaces within the logistics sector. These standards enable corporations to exchange essential transport and freight information with government agencies in real-time, lowering administrative costs and improving operational efficiency (European Commission, 2020). For example, freight operators can now electronically lodge digital consignment notes with customs, which enhances the efficiency and accuracy of customs clearance. In this, B2B and B2G communications are supported by interfaces such as Port Community Systems (PCS), which allow real-time data sharing between shipping companies, customs, and logistics providers (Chountalas et al., 2024).

For truckers, G2B solutions such as Truck Appointment Systems (TAS) and intelligent road infrastructure are being introduced to make good movement more efficient and minimize congestion in terminals and seaports (Lange et al., 2022).The systems permit truck arrivals to be pre-reserved, whereby there is minimal waiting time and more efficiency in cargo handling. Besides, technologies such as Geofencing and RFID are enhancing visibility in operations, and companies are finding it easier to track vehicles and cargo (Dasaklis et al., 2024). Information security remains an issue here, however. Increased exchange of digital data between firms and government agencies requires the implementation of secure data transmission protocols, encryption technology, and compliance with cybersecurity standards (Heilig & Voß, 2016).

Over the long term (5-10 years), B2G and G2B transactions will be a completely different thing with much greater integration of Intelligent Access (IA) technologies and smart infrastructure. IA technologies, which imply using digital technology to have the correct vehicle on the correct road at the correct time, will make the fullest possible use of the road, prevent traffic jams, and make road travel safer (European Commission, 2020)

Road hauliers will see greater automation of traffic management in the future, where AutoTRIX and Geofencing systems offer more sophisticated traffic control and fleet management (Jacobsson et al., 2020). These systems will help in providing smoother coordination between companies, government agencies, and other stakeholders in road freight transport.
In regards to information standards, the eFTI and eCMR standards will be fully incorporated into the logistics value chain to enable seamless cross-border data exchange and minimize the time gap in connection with paperwork and regulatory processes (European Commission, 2020). Governments will apply such digital standards to make it easier to process transport documents and ensure that compliance is easily accessible. Intelligent roads and intelligent parking facilities will also be advanced with integrated systems that can track vehicles in real-time, manage traffic, and maximize the utilization of parking space (Lange et al., 2022).
With extensive deployment of these technologies, information security will increasingly play a vital role. With more online information being exchanged among business and government communities, the integrity and confidentiality of such information will require strong cybersecurity measures, including encryption, data secure storage, and authentication (Heilig & Voß, 2016). Moreover, blockchain technology can potentially play an instrumental role in rendering data exchanges tamper-proof, providing greater security to sensitive freight and transport data (Dasaklis et al., 2024). These technologies will render freight and logistics processes more efficient, secure, and eco-friendly, propelling a more automated and networked global supply chain.

2.4.6 DATEX II

The DATEX II standard is presently a principal facilitator for real-time and interoperable data exchange between European transport systems, precisely enabling Intelligent Access (IA) applications for road freight and terminal-port logistics. Initially developed to enable common communications between traffic control centers, DATEX II has progressively been broadened to embrace urban mobility, roadworks, parking, environmental monitoring, and automated driving (DATEX II, n.d.-a). Its multi-part specification based on modular construction enables dedicated application across use cases. Notably, Part 6 (CEN/TS 16157-6:2015) concerns truck parking data, offering metadata regarding availability, infrastructure services, and user authorizations relevant to logistics access planning (Melo-Castillo et al., 2017). It also accommodates static and dynamic data, such as occupancy and geospatial access prohibitions, enabling real-time, criteria-based decision-making on access responsive to the operational goals of IA (Delgado et al., 2024). Its profiling ability also enables implementers to create lean, application-specific subsets of the standard, reducing data complexity without sacrificing necessary interoperability (DATEX II, n.d.-b). Notably, as per Directive 2010/40/EU, DATEX II becomes mandatory for EU National Access Points (NAPs), further establishing itself as the key harmonized traffic and freight data exchange standard (European Commission, 2010; DATEX II, n.d.-c).
Apart from its current applications, DATEX II will be vital in future IA system development. Initiatives such as the LOD-RoadTran18 project have brought DATEX II to the Linked Open Data (LOD) level and provided semantic meaning to its data that facilitates integration with cross-sectoral information environments more effectively (Delgado et al., 2024). This semantic transformation in the form of LOD-DATEX is not only facilitating reusability of data but also allowing greater interoperability with data sets of application domains such as environmental policy, multimodal logistics, and smart cities. DATEX II is also expanding the standard's application to cooperative, connected, and automated mobility (CCAM), electromobility infrastructure, and digital traffic legislation—all new data-driven freight and access control system priorities (DATEX II, n.d.-a). With these expansions ongoing, DATEX II will enable increasingly intelligent, autonomous access mechanisms in which use of the infrastructure is regulated by dynamic conformity to vehicle-specific,

temporal, and spatial conditions. These are complemented by longer-term strategic IA objectives several years in the future for safety, sustainability, and infrastructure optimization and make DATEX II not only a short-term solution but also a visionary standard.

2.4.7 National Access Points (NAP)

In the current European transport ecosystem, the role of National Access Points (NAPs) as the backbone of Intelligent Transport Systems (ITS) particularly in road freight and port-terminal logistics is worth noting. Established through the ITS Directive 2010/40/EU and implementing regulations (EU) No. 885/2013, 886/2013, 962/2015, and 1926/2017.NAPs are described as the central digital resources that support the storage, processing, and exchange of data within the transport network (European Commission, 2024). These platforms form the foundation for the whole data stakeholders' e.g. infrastructure entities, service providers, and public authorities, the coordination of a harmonized set of data used to improve traffic monitoring, route planning and scheduling of freight transport.

The operational NAPs are currently the case in most of the EU member states. There are countries like Germany (Mobilithek), Austria (mobilitydata.gv.at), and Belgium (transportdata.be) with the working systems that support multimodal travel information, real-time traffic data, and safe parking availability (European Commission, 2024; TRA, 2022). These can be both the centralized data repositories and the federated access points themselves that are using metadata standards such as DCAT-AP and DATEX II to make sure that semantic interoperability is achievable (Mylonas et al., 2023). NAPs in the port-terminal logistics case, make it possible to have the Port Community Systems (PCS) and Transport Management Systems (TMS) aligned, the accuracy of arrival, cargo information, and slot checks are made higher with this system.

Challenges are still around in the wake of this progress. The existing NAP ecosystem is hindered by architecture divergence, lack of complete datasets, and sporadic coverage of EU-mandated quality and metadata protocols (Hendriks et al., 2018). Nonetheless, even if Delegated Regulation 2017/1926 requires, at present, immediate and historical data dissemination through NAPs, a lot of discrepancies still abound especially in the sectors of dynamic data for instance predictive traffic analytics or freight congestion alerts (European Commission, 2024). The NAPCORE initiative is making attempts to bring about the harmonization of metadata vocabularies and reporting templates in Member States (NAPCORE, 2022).

The current timeframe for these deployments has been stressed by the European Green Deal ambition, aiming at a 90% emission reduction by 2050, thereby placing ITS and digital platforms at the core of achieving climate neutral logistics (EPRS, 2021). Consequently, NAPs are no longer mere mechanisms of compliance; they are strategic assets to engineer freight efficiency and mitigate environmental externalities in the short term.

It can be quite rightly predicted that in the future National Access Points will surely go through major changes in their functions. The functions will not only be transformed from data intermediaries into smart mobility data systems but will also have the intelligent capability. Up to ten years from now, the integration of NAPs will have become so pronounced that they will have merged with Cooperative Intelligent Transport Systems (C-ITS), Mobility as a Service platforms, and autonomous freight management systems (Mylonas et al., 2023). The NAPs of the coming years will heavily rely on machine-readable, real-time and predictive data formats that not only humans but self-governing logistics fleets and port robots may benefit from.

The enrichment of the napDCAT-AP standard is going to be one of the most critical strides, i.e. with the development of the domain-specific extension to DCAT-AP covering the NAPCORE program. The NAPCORE program is the source of this extension. There will be specific metadata profiles for the use cases of freight transportation, such as geospatial truck positioning, emission zones, and cross-border permit validation (NAPCORE, 2022). Moreover, as the digitalization process grows, NAPs will not only serve as a place to start building up but a solid foundation upon which to set up virtual traffic management centers, safety observatories, and disaster response systems will be established. In turn, all these resources will enable quicker re-routing, access prioritization, and risk management in logistics (Mylonas et al., 2023).

Refinements in the legal framework are to be expected and they are set to match the aforesaid technological revolution. The recently legislated MMTIS Delegated Regulation, also numbered EU 2024/490, already contains so many stipulations that are yet to be understood by the Member States in the EU. This regulation has now been revised. The final draft outlines the new imposition on all Member States to contribute to the Multimodal Traveler Information Service (MMTIS) regulation (European Commission, 2024). By that time NAPs will have got used to compliance checks being done automatically, they will have even got contracts that are smart and provide secure APIs for data trust and data exchange in freight corridors. The latter will be achieved by using the latest cryptographic algorithms like JSON Web Signature (JWS) although this will be in addition to decentralized digital identities.

In addition to NAPs becoming federated nodes in the pan-European mobility data space, the European Commission aims at these platforms not to work independently at the national level but as a cluster of networked devices. This will be made possible by the support of real-time access control, congestion pricing, and carbon tracking at the logistics corridor level (EPRS, 2021).

2.4.8 Eurostat

Eurostat, the EU statistical office, offers harmonized transport statistics critical for policy-making and cross-border analysis (Eurostat, 2022). In road transport, which constitutes over 70% of freight transport and 80% of passenger transport in the EU, Eurostat supports the European Green Deal and the Trans-European Transport Network(TEN-T) policies via standardized high-quality dataset provision (Eurostat, 2022; European Commission, 2020).

Statistics are gathered by national offices via NACE classification and include key economic indicators like turnover, employment, and investments (Eurostat, 2000). The functional areas of Eurostat track mobility, emissions, and fuel usage (Eurostat, 2000). In cooperation with DG Regional Policy, Eurostat further estimates accessibility to transport via grid-based population coverage measures in 90 minutes, which reveals spatial differentials between nations (Dijkstra, Poelman, & Ackermans, 2019). They are used extensively in all EU and EFTA member states and serve as a foundation for policy-driven transport decisions (Eurostat, 2022).

Over the coming decade, Eurostat will move to real-time and dynamic data integration as per the incoming smart mobility, autonomous transport, and digital freight networks (Eurostat, 2022; European Commission, 2020). The future method will utilize telematics, IoT sensors, and predictive analytics to monitor road usage and environmental impact in real-time (Eurostat, 2022).

Accessibility models will be revolutionized from inflexible 90-minute measures into congestion-sensitive, predictive ones to facilitate more data-driven infrastructure planning (Dijkstra et al., 2019). Integration with digital standards such as eFTI and eCMR will create interoperability of

data among logistics platforms (Eurostat, 2022). It will be rolled out by 2030–2035, depending on Member States' digital readiness (Eurostat, 2022). The future role of Eurostat will be at the forefront of coordinating smart, green, and connected EU transport networks (Eurostat, 2022).

2.5 Information Systems in Road Freight Transportation and Port and Terminal Logistics

Information systems provide the core from which PCS, TMS, FMS,TAS,TOS and ERP are instituted in the processes for optimizing logistics in ports and terminals.

2.5.1 Port Community Systems (PCS)

Currently, Port Community Systems (PCS) are centralized digital systems that support information flow among the stakeholders. In these systems, shipping lines, customs authorities, port authorities, and logistics service providers are able to share information in a standardized format (Heilig & Voß, 2017). These systems allow for integration and digitization of core processes, including real-time container tracking, vessel scheduling, and customs clearance (Tijan et al., 2014). PCS diminishes administrative overheads, maintains data integrity, and improves operational transparency (Tijan et al., 2021). Integration with Terminal Operating Systems (TOS) and national customs platforms allows dynamic berth scheduling and greater facilitation of trade (Perego et al., 2021).

PCS will develop into inter-operable ecosystems wherein real-time interaction and seamless data transfer will be possible across borders (Rodon & Ramis-Pujol, 2006). With further optimization of port logistics using cloud infrastructure, artificial intelligence, and automated workflow engines, these platforms will sync supply chains and break down information silos while responding to disruptions and market changes (Heilig & Voß, 2017). Future PCS will be characterized by a socio-technical system design that balances technical resources with organizational human settings for optimum results (Tijan et al., 2021).

2.5.2 Transportation Management Systems (TMS)

Digital transportation management systems are the backbone of transportation logistics (Drljača & Sesar, 2023). Nowadays, they manage routing, dispatching, shipment tracking, and cost optimization in a multimodal environment (More et al., 2022). It integrates with other enterprise systems and provides web-based services, such as real-time dispatching updates, digital document storage, and performance analytics (More et al., 2022). The TMS has recently played a crucial role in improving on-time delivery, reducing the costs of transportation, and enhancing customer satisfaction (Drljača & Sesar, 2023).

Next-generation TMS will introduce ontological modeling and enterprise alignment frameworks such as Zachman for custom configuration based on an organization's semantics (Dorofeev et al., 2020). They will be AI- and machine-learning-driven, maintaining dynamic routing, predictive analytics, and automated vendor selection (Dorofeev et al., 2020). In time, they will transform into smart platforms that will assist the business in operational efficiency and contribute to strategic decision-making (More et al., 2022).

2.5.3 Fleet Management Systems (FMS)

FMS technologies empower the logistics company in monitoring the health, location, fuel usage, and driving patterns of vehicles through IoT devices and mobile applications (Shivkumar & Supriya, 2024). Such systems provide the fleet managers with real-time updates that can lead to preventive

maintenance and reduced downtime for vehicles (Challa, 2016). Platforms like ThingSpeak cloud for integration of GPS and telematics are engaged for optimizing the delivery routes and asset utilization (Shivkumar & Supriya, 2024).

FMS is heading toward a centralized leasing and management model with a focus on reduced fleet size, operational costs, and higher standardization (Kunz et al., 2015). AI-assisted diagnostics and cloud-based dashboards will be an integral feature of the systems of the future for predicting maintenance, optimizing fuel consumption, and creating an in-depth analysis of driver behavior (Shivkumar & Supriya, 2024). These updates will lead to sustainable and resilient logistics operations (Kunz et al., 2015).

2.5.4 Truck Appointment System (TAS)

The TAS provides booked time slots for trucks so that truck arrivals at ports and terminals may be facilitated (Im et al., 2021). This scheduling reduces congestion, improves yard operation, and minimizes carbon emissions from idling trucks (Lange et al., 2022). It's usually rigid in its current form, with little integration into the operational constraints of trucking companies (Phan & Kim, 2016). It also operates on a first-come, first-served basis, which limits its flexibility (Ericsson & Svensson, 2022).

Collaborative TAS models will allow iterative exchange of preferences between trucking companies and terminal operators (Phan & Kim, 2016). Estimated waiting times and yard congestion feedback will allow endless and dynamic adjustments of appointments (Phan & Kim, 2016). Such systems will promote flexibility, improve overall throughput, and gain acceptance by aligning with stakeholders' operational realities (Ericsson & Svensson, 2022).

2.5.5 Terminal Operating Systems (TOS)

However, TOSs are the fundamental software systems that run the cargo operations in port terminals (Min et al., 2017). The system supports real-time container flow, berth planning, and inventory management (Choi et al., 2003). The fast turnaround of ships and efficient yard planning is contributed by modules such as Electronic Data Interchange (EDI) and automated billing (Min et al., 2017). AI is now being used to predict congestion, optimize container placement, and improve equipment allocation (Zimmerman et al., 2021).

The future TOSs will operate in distributed combined heterogeneous network environments with intelligent mobile terminals (Koutsorodi et al., 2006). Advanced modules such as Mobility Management and Network Interface Adaptation will ensure accessing cellular, Wi-Fi, and broadband networks concerning their Quality of Services and costs (Koutsorodi et al., 2006). Completely integrated and standardized systems will open up the silos of data and make possible collaborative planning between terminals and supply chain partners (Min et al., 2017).

2.5.6 Enterprise Resource Planning (ERP)

In the contemporary ERP systems, business functions finance, procurement, HR, and logistics are tied together into the same system (Aremu et al., 2018). They help to share data in real-time and facilitate global deployment through cloud-based solutions (Ebirim et al., 2024). In logistics, ERP controls customs documents, warehouse operations, and cargo tracking (Aremu et al., 2018).

Future Scenario(5-10 years)
AI integration, machine learning, IoT, and blockchain will transform ERP (Alaskari et al., 2021). Thus, these changes will turn ERP into an intelligent decision-making system capable of optimizing real-time activities and undertaking predictive maintenance (Kłos et al., 2021). Strategic dashboards will then prove insights into cost control, asset reliability, and supply chain performance, thus elevating ERP for administrative to strategic applications (Kłos et al., 2021).

2.5.7 Intelligent Transport Systems

Intelligent Transport Systems (ITS) refer to new applications involving information and communication technologies (ICT) that are now revolutionizing logistics and road freight transport (Hasan, Siddique & Chakraborty, 2013).ITS is an umbrella term consisting of advanced applications designed to improve traffic management, operability, and also sustainability by improving the communication and information flow between vehicles, infrastructure, and logistics centers (Hasan et al., 2013).
It is keeping pace in contemporary road freight transport with dynamic routing, vehicle tracking, real-time traffic updates, and logistics management (Hasan et al., 2013).These systems help alleviate congestion; improve fuel efficiency by coordinating vehicles; and enhance delivery reliability (Hasan et al., 2013).Technologies like GPS and Wireless Local Area Networks (WLANs) enable constant communication between vehicles and traffic management systems, thus ensuring the efficient management of freight transport operations (Hasan et al., 2013).Real-time monitoring of vehicle location, cargo conditions, and operational statuses leads to increased transparency in logistics and improved decision-making (Hasan et al., 2013).ITS have also supported port terminal logistics with automated handling of containers, real-time tracking, and gate management systems (Perallos et al., 2015).Port terminals are now deploying Radio Frequency Identification (RFID), Automated Guided Vehicles (AGVs), and integrated Terminal Operating Systems (TOS) to enhance loading and unloading procedures, minimize turnaround times, and achieve optimum resource utilization (Perallos et al., 2015).ITS also involves dedicated short-range communications (DSRC), which will provide efficient vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication (Williams, 2008).DSRC ensures high-speed low-latency communication that is crucial in promoting road safety, avoiding collisions, and managing traffic congestion in an efficient manner (Williams, 2008).In-road truck platooning, where trucks are conveyed closely under their control systems, greatly contributes to fuel economy and emission reductions, with trials already being undertaken in several regions (Williams, 2008).
Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Vehicle (I2V) communication technologies play significant roles in modern intelligent transport systems because they greatly enhance efficiency, safety, and environmental sustainability for road transport and port terminal logistics (Williams, 2008). The V2V communication techniques today are capable of enabling the direct connection and interaction among vehicles to exchange relevant safety and operation information that concern collisions and the general flow of traffic (Dey et al., 2016). Examples of today's V2V applications are cooperative collision warnings, lane-change assistance, a blind-spot detection, and platooning, in which vehicles travel in close-in groups, which significantly improves fuel economy as well as traffic management (Williams, 2008).
Vehicle-to-Infrastructure (V2I) communication has actually given new dimensions in the operations of vehicles that interact directly with road infrastructure, selecting routes most efficiently, hence decongesting traffic and lowering idling levels, achieving best environmental performances (Dey et al., 2016). Some modern practical applications of V2I are intelligent traffic signal systems, dynamic speed limit advisories, and automated tolling; together, these improve the flow of traffic while minimizing operational hold-ups (Williams, 2008). Infrastructure-to-Vehicle (I2V) is where

infrastructure nodes actively send their critical responses or updates to vehicles, including hazardous traffic incidents, ambient conditions, and all the dynamic advisories needed for operational safety and efficiency (Pathak & Shrawankar, 2009). Currently, with the assistance of I2V applications, vehicles are capable of navigating complex port and logistic terminal environments through automated gate access, hazard warnings, and precise instructions regarding the handling of cargo that significantly reduces manual errors and delays (Pathak & Shrawankar, 2009).
In fact, today's scenarios are already demonstrating the dividends that accrue from such technologies, including intelligent evacuation systems, logistics coordination during emergencies, and next-generation traffic management systems (Hassan et al., 2023).

By looking into the future, IT shall significantly expand due to new developments like Cooperative Intelligent Transport Systems (C-ITS) (Williams, 2008).These cooperative systems will enhance the predictive analytics, proactive management, and autonomous operation ability of vehicles, the infrastructure, and the logistics hubs, by permitting mutual real-time data exchange (Williams, 2008).These expected autonomous trucks within ITS networks will further optimize the logistics operations and thus mitigate human errors, enhance safety, and help to significantly reduce operating costs (Williams, 2008).
Implementation of AI and ML would be significant for future advancement in ITS to allow advanced data analysis, traffic prediction, and automated decision-making. AI-enhanced predictive analytics can foretell traffic congestion, mechanical failures, or even predict logistics demand patterns, providing substantial operational planning and resource allocation benefits (Perallos et al., 2015).Integration of blockchain technology into ITS offers an interesting opportunity for elevating supply chain transparency, safety, and traceability(Bakhtina, Matulevičius & Malina, 2024).The immutable ledgers of blockchain render a secure, transparent, and tamper-proof record of transaction traces that significantly enhance customs clearance-related activities, cargo authenticity verification, and documentation management in freight logistics (Bakhtina et al., 2024).ITS will greatly promote environmental sustainability by providing technical expertise for emissions and energy consumption management (Williams, 2008).Advanced systems capable of real-time route optimization based on environmental factors, traffic status, and energy efficiency will greatly reduce the ecological footprint of road freight transport and port activities (Williams, 2008).However, cyber security and data privacy are among the numerous challenges confronting ITS expansion and integration into logistics (Bakhtina et al., 2024).The level of connectivity and interdependence of transportation systems will raise the level of risk relating to cyberattacks and data breaches (Bakhtina et al., 2024).Establishing cybersecurity mechanisms that meet strict standards for information security like ISO/IEC 27001 and privacy- compliance to regulations like the General Data Protection Regulation (GDPR) should be the foremost consideration safe and effective ITS deployment(Bakhtina et al., 2024).

Innovative V2V communication technologies in the future will enable fully autonomous vehicle coordination such that all vehicles will be capable of platooning, automated collision avoidance, and highly coordinated lane management systems (Hassan, Wolshon & Sultana, 2023). Cooperative algorithms developed will advance real-time exchange of data between vehicles, by the dimension of such communication, the traffic management will be further improved as well as risk reduction of accidents (Dey et al., 2016).
The trend of V2I communications would include artificial intelligence and big data analytics, enabling the infrastructure dynamic to respond itself to varying traffic conditions (Stavropoulos et al., 2012). It will feature real-time adaptive traffic signals on I2V systems; personalized route recommendations based on predicting modeled havoc congestion; automated, infrastructure-driven vehicle guidance

systems, and operational efficiency optimizations with reduced environmental impact (Dey et al. 2016).
Infrastructure-to-Vehicle communication is going to be further realized through the inclusion of multimedia and real-time video communications which are going to provide vehicles with accurate context-based advisory information (Perallos et al., 2015). Future I2V applications can be imagined as advanced alerts for predicting hazards, automated handling of more detailed and precise logging of logistical operations, and fully automated gate access systems for interacting with complex logistical environments, such as ports (Pathak & Shrawankar, 2009).
Certainly, for the best benefits possible from these technologies in the future, it is imperative that wireless communication standards are continuously improved, particularly for high-speed, low-latency interactions such as with the IEEE 802.11p standard (Hasan, Siddique, & Chakraborty, 2013). The systems of ITS which are crucial to high-density logistics operations and emergencies will then be robust and reliable (Hasan et al., 2013).
Future setting scenarios would lead to an exhaustive integration of V2V, V2I, and I2V technologies, thus transforming the transport ecosystems into fully connected, automated, and intelligent transport ecosystems. This phenomenon will significantly affect logistics and transport businesses, setting new standards for operation efficiency, reliability, safety, and environment stewardship (Williams, 2008).

2.5.8 Geofencing in Road Freight Transport and Port/Terminal Logistics

In today's logistics environment, geofencing is being used as a tactical measure to improve operational visibility and cargo security in road freight and port logistics. In road freight, geofencing enables real-time tracking, route compliance, and unauthorized access detection through the combination of GPS technologies with RFID and mobile communication systems (Oliveira et al., 2015). Technologies such as SafeTrack illustrate how geofencing can automate delivery confirmation and notify dispatchers of deviations or suspected thefts, drastically minimizing dependence on manual surveillance. In port and terminal logistics, geofencing is being combined with RFID and terminal operating systems (TOS) to initiate automated gate access, synchronize check-in/check-out operations, and track yard activities. These applications are typically implemented in controlled environments, such as closed pilot schemes in urban freight zones in cities such as Stockholm and Gothenburg (Lindkvist, Lind, & Melander, 2023), where geofencing enables electric vehicle mode switching, speed enforcement, or restricted zone entry.

In spite of such promising applications, mass adoption is still limited by technological and organizational fragmentation. Both public and private interests lack agreed standards for specifying geofence parameters, sending geolocation messages, or interoperating geofencing with pre-existing ITS infrastructures (Lindkvist et al., 2023). Furthermore, the roles of the stakeholders—municipalities, motor vehicle manufacturers, and logistics services providers—remained indeterminate and, in some instances, undefined, in terms of ownership of data, duty of enforcement, and interoperability. The issues point toward more transparent government structures and, more importantly, the establishment of common data standards for geofencing applications within freight transport (Melander, Lind, & Lindkvist, 2021).

During the next decade to fifteen years, geofencing will move from an add-on control measure to a fundamental part of intelligent access management for multimodal logistic networks. With digital platforms and standardization structures (e.g., GS1 EPCIS, ITS standards) maturing, geofencing will be implemented along supply chains, with open vehicle-to-infrastructure (V2I) and system-to-system exchange (Oliveira et al., 2015; Lindkvist et al., 2023).In trucking freight, geofencing would not only

have to adhere to routing and delivery policy but also dynamically re-route in real time due to congestion, environmental areas, and risk considerations. Trucks would automatically react to geofence events change in speed, driving mode, or stopping at virtual check points—according to pre-authorized access profiles.

In terminal and port operations, geofencing will allow "smart gate" systems to communicate directly with digital twin spaces and AI-driven scheduling engines. This will facilitate full automation of coordination of trucks, containers, and equipment, optimizing time slots, safety zones, and terminal throughput. Moreover, as geofencing is paired with blockchain or secure cloud platforms, it will be part of auditable, trusted event streams shared between customs, port authorities, and third-party logistics providers (Melander et al., 2021). Actor roles will also be redirected toward long-term interoperability: public authorities will be custodians of data and facilitators of policy, while private actors will be integrators of services and operators of platforms. This will be a transition from firm-centric to network-centric innovation (Guercini, Lind, & Melander, 2022), enabled by collaborative governance models and shared incentives toward sustainable, efficient logistics. But such a future rests crucially on synchronizing investment in digital infrastructure with harmonization of the regulatory environment and data-sharing terms. In the absence of open standards for role allocation, access control, and system integration, the potential of geofencing in intelligent access systems may go unrealized. Promoting open standards and multi-actor interoperability is hence an essential pre-condition for the future of geofencing innovation in freight transport systems

2.6 Data Security

The protection of digital data in sea ports and terminal logistics is, indeed, mandatory, because with such measures in place the information will not be obtainable by unauthorized parties. Operational continuity will be ensured along with compliance with international-level regulations. It will also act as a defense against threats emanating from unauthorized data access, data breaches, or cyberattacks.Data Governance Frameworks (DGF) establish policies concerning data integrity, flow rules, permissions for access, and security. They are important in an environment that is dynamic and characterized by multiple stakeholders, where an information asymmetry is possible. The Data Governance frameworks will make sure that safe collaboration on data exchange will be possible between the stakeholders while the risk of possible breaches will be avoided (Wang & Li, 2020).

2.6.1 Intelligent transport systems as Information security

Currently, ITS data security is highly important now as the exchange is sensitive between vehicles and infrastructure, which involves logistics centers (Bakhtina et al. in 2024).Protection of data integrity, confidentiality, and availability of present ITS goes with an efficient cybersecurity mechanism such as encryption, authentication mechanism, and intrusion detection system (Bakhtina et al., 2024).Confidentiality refers to ensuring that sensitive data, such as delivery scheduling information, driver information, and cargo manifests, will not be accessed by any unauthorized people (Bakhtina et al., 2024). Integrity ensures that the data is just as accurate and unchanged during transmission, which is very important for effective decision-making and logistics planning (Komar, 2024). Availability ensures continued access to ITS services, which are critical for logistics and port usage (Bakhtina et al., 2024).Compliance with the international security framework of ISO/IEC 27001 can organize, manage, and protect sensitive data from possible risks by cyber attack, data breach, or unauthorized access.Areas for frequent security audits, penetration tests, and continuous practices of monitoring were set up to ensure that security loopholes within ITS infrastructures are identified and rectified promptly (Bakhtina et al., 2024).ITS networks mostly suffer from the condition of interoperability

along with requiring standardized protocols for ensuring data sharing in a secure manner between various stakeholders (Komar, 2024).

As ITS data security will not only become part of the norm but also part of a chain of consequences in the future scenarios because those systems are widely interlinked and automated. These will be developed by new technologies such as quantum cryptography, blockchain as a secure means for data transaction and complex AI driven systems for detection of emerging threats, which will constitute the core components of future ITS cybersecurity strategies (Bakhtina et al., 2024). Future architectures, such as the new and improved ISO/IEC 27001 standard and the NIST Cybersecurity Framework 2.0, will encompass the holistic guidelines that may be valuable in securing ITS against complex and continually evolving cyber threats (Bakhtina et al., 2024). Proactive cybersecurity measures, such as advanced anomaly detection, predictive cybersecurity analytics, and automatically invoked incident response measures, will be integrated into the daily operations of ITS management (Bakhtina et al., 2024).
Trends in the future for security in ITS include using blockchain technology and multi-party computation (MPC). Through blockchain technology, decentralized and secure transactions can be recorded with transparency across logistics systems that could help address some security concerns in the supply chain, including cargo tracking and customs documentation (Bakhtina et al., 2024).
Multi-party computation allows secure collaboration and analytics with respect to sensitive data without losing individual privacy (Bakhtina et al., 2024).
Homomorphic encryption and attribute-based encryption are cryptographic approaches that will improve privacy through protecting sensitive information while allowing data processing (Bakhtina et al., 2024). Privacy-enhancing technologies (PETs) such as anonymous authentication and anonymous credential systems ensure anonymity for both driver and passenger, hence minimizing risks relating to the misuse of personal data (Komar, 2024).
Security training keeps on being very vital and stresses educating on identifying and responding to cyber threats for all stakeholders involved in logistics and transport operations(Bakhtina et al., 2024). Continuous staff training ensures resilience against common cyber threats, including phishing and ransomware attacks prevalent in transportation sectors (Komar, 2024).

Encryption technology is generally used in ports to secure data while being transmitted from one port-related system to another. Sensitive information, such as customs documents and cargo manifests, is visible only to authorized parties (Heilig & Voß, 2016).Role-based access control (RBAC) is concerned with limiting access on systems according to the particular user role and responsibility. It ensures that only authorized personnel can have access to view or modify sensitive data (Wang & Li, 2020).New blockchain technology will provide the stakeholders with a decentralized, tamper-proof, and immutable ledger that prevents tampering and unauthorized modifications from possible intrusion (Heilig & Voß, 2016).Ports are observed to conform to international standards. Their compliance with international standards includes the International Maritime Organization (IMO) guidelines on cybersecurity and ISO 27001 for information security management (Heilig & Voß, 2016).

2.6.2 RFID and EDI as Information Security

RFID also has an important role in safeguarding information security in supply and logistics activities. Because RFID necessitates sending out sensitive data shipment status, cargo goods, and shipment timetables the data need to be kept safe to discourage others from misusing the data, and so integrity is not tampered with. One of the major processes protecting RFID information is encryption such that

information reaches the hands of and is operated only by permissible systems and end users(Shi et al., 2011).
Besides encryption, data integrity measures like error-checking algorithms are used to guarantee that the information read and transmitted by RFID systems does not get corrupted during transit. Such security measures are especially crucial in settings where there is a need for real-time tracking and monitoring of commodities, like at ports or warehouses where commodities are moving about and interacting with different systems. Through the integration of these security features, RFID technology mitigates the risks of data breaches and fraud while ensuring the confidentiality and integrity of the information transferred between systems.(Imburgia, 2006).

EDI also has a critical function in information security in that it helps to ensure that data exchanged between organizations is safe from unauthorized access and tampering. EDI systems usually use secure communication protocols, like Secure Sockets Layer (SSL) or Transport Layer Security (TLS), to encrypt the data being sent over the network. These encryption protocols help to ensure that sensitive data, like financial transactions or shipping information, is safeguarded during transmission(Shi et al., 2011).

Furthermore, authentication mechanisms are employed in EDI systems to authenticate the identities of the receiver and sender so that the data is being shared between legitimate persons. This provides an extra layer of protection to prevent unauthorized users from accessing sensitive information. Through the incorporation of these security attributes, EDI technology ensures that data shared between companies is protected against data breaches or fraud(Imburgia, 2006).

Over the next decade, RFID use in port and logistics facilities will be driven by increasingly advanced data security systems. As RFID becomes a foundation of real-time visibility into goods, worker safety, and asset tracking, it also presents risks of wireless data transmission, tag cloning, and unauthorized reading.

To counter these threats, the second generation of RFID deployments will be incorporated into Zero Trust Architectures (ZTA) and multi-layered encryption architectures, where each and every data exchange tag, reader, and back-end system is authenticated and vetted (Bauk, Schmeink, & Colomer, 2018). Next-generation RFID systems will be designed on end-to-end encryption, tokenization, and machine learning-driven anomaly detection algorithms to scan and mark abnormal behavior in real-time.

Apart from that, blockchain integration with RFID will be at the forefront to solve the problem of data traceability and immutability.Blockchain-ledgers will hold RFID-collected events such as container access or movement of location, with tamper-proof audit trails and verifiable user and asset identities (Wang et al., 2021). Security standards such as ISO/IEC 29167, which provides guidance on cryptographic suites used in RFID, will continue to evolve and integrate itself with GDPR, NIS2, and future AI liability directives in the EU and other nations.

While Electronic Data Interchange (EDI) has long facilitated structured supply chain communication, its security architectures have thus far been rigid, perimeter-defense based. In the next few years, EDI will be transformed by the need for secure, interoperable, and resilient data exchange in complex, multi-actor ecosystems.

As EDI moves to cloud-native and API-based platforms, data security architecture will shift to identity and access management (IAM), digital signatures, and real-time encryption to safeguard

sensitive trade documents like bills of lading, invoices, and customs declarations by securely storing and sharing them (Imburgia, 2006). ISO/IEC 27001 and NIST Cybersecurity Framework (CSF) will increasingly be utilized as starting points to manage data confidentiality, integrity, and availability.

In addition, interoperability among other secure protocols, such as RFID-based IoT data streams, will require data validation schema standardization, message authentication codes (MAC), and public key infrastructures (PKI). Conformance will become more stringent, and audit-ready systems will be required to show not only encryption but data provenance, consent capture, and risk-based access control.

Converging EDI and RFID will meet in Secure Digital Logistics Platforms, where real-time sensor data, transactional messages, and identity credentials are integrated under shared cybersecurity measures. Convergence will increase supply chain resilience, diminish fraud, and provide legal traceability of goods and data across borders (Inkinen, Helminen, & Saarikoski, 2019).

2.6.3 AMS Framework

The AWS Managed Services (AMS) system offers strong security solutions, which are most critical for road freight transport and port terminal logistics. AMS strengthens information security practices due to the sensitivity of the data in the fields, for example, shipment details, cargo manifests, routing data, and payment particulars.AMS provides an advanced endpoint security solution, where the system combines anti-virus and anti-malware technologies to protect IT systems that support logistics operations from threats actively (Amazon Web Services, Inc., 2025). Main tools introduced from AMS are Amazon GuardDuty and AWS Security Hub for security threat detection and intrusion prevention, which helps to lower the risk of potential security breach.

AMS implements continuous monitoring, logging, and alerting for security purposes through the use of Amazon CloudWatch and AWS Config. This set of services detects anomalies and suspicious activities in the managed environment and promptly raises alerts to teams with indications or threats to security(Amazon Web Services, Inc., 2025). Rapid detection and response capabilities like these are vital in every logistics firm in maintaining operational integrity by mitigating risks before they escalate into serious threats.

AMS puts in place a very elaborate and orderly change management system that tightly governs all changes to the infrastructure according to agreed request-for-change (RFC) procedures, so that only authorized interventions are allowed to take place. This way, it looks after the integrity of ports and transport infrastructure against careless vulnerabilities (Amazon Web Services, Inc., 2025). IAM within AMS provides highly controlled access to resources, networks, or data within logistics environments. AMS controls the processes used to authenticate users and grant permissions against the unauthorized access to data, so that sensitive information-regarding for example cargo tracking and port operational data-is kept secured (Amazon Web Services, Inc., 2025).

AMS also follows prescribed compliance, and the compliance requirements considered for managed environments are continuously verified. AWS Security Hub, Amazon GuardDuty, and Amazon Macie are the compliance framework tools used to help automate security threat and data leakage detection and response, thereby protecting logistics operations from compliance violations and security breaches (Amazon Web Services, Inc., 2025).

AMS performs proactive patch management against vulnerabilities to ensure system safety. Periodic updates fortify the infrastructure against known security risks while minimizing the impact of

potential cyber threats and conspiring against the uninterrupted flow of logistical operations (Amazon Web Services, Inc., 2025).

In the future, AMS is likely to extend intelligent access and security management with incorporation of artificial intelligence and machine learning (AI/ML) into its security architecture. These techniques will boost detection capabilities, allowing for predictive analytics to identify vulnerabilities and cyber threats even before they occur (Croma Campus, 2024).

AMS is likely to further advance compliance automation by integrating more sophisticated compliance tools and increasing regulatory coverage that would ensure seamless adjustments to changing global standards (Croma Campus, 2024). The future AMS security framework could employ advanced biometrics and blockchain technology for identity validation and transaction management, especially in logistics where it helps with the secure verification of drivers and operators, significantly reducing the risks of unauthorized access (Croma Campus, 2024).

In addition, IoT (Internet of things) integration within the AMS security ecosystem should allow for the real-time tracking and protection of logistics assets, ensuring that each endpoint and network component remains secure against threats emerging in an ever-connected environment (Croma Campus, 2024).

In these advances, AMS would retain its full capabilities in providing a comprehensive, adaptive, and future-ready information security solution for road freight transport and port terminal logistics (Croma Campus, 2024).

2.6.4 Zero Trust Architecture

Zero Trust Architecture (ZTA) is a comprehensive security architecture that continuously checks for user and device legitimacy while granting minimum access levels to eliminate modern threats to information security. ZTA is a vital application in road freight transportation and logistics, where real-time data sharing, exact vehicle tracking, and dynamic optimization of routes are the lifeblood. As said, ZTA provides credible, reliable access to sensitive data, significantly reducing the risk of any form of cyber threat and unauthorized access (Kulkarni & Cheikhrouhou, 2024).

ZTA can be married to these telematics and IoT technologies, thus ensuring continuous authentication and real-time monitoring under the more comprehensive umbrella of advanced security and operational awareness. Under this new arrangement, Intelligent Transport Systems (ITS) significantly benefit through developing the monitoring of vehicle and cargo conditions through the use of multiple sensor varieties that are recognized under ZTA. This protects sensitive logistics from unauthorized tapping, resulting in a higher state of operational security and reliability (Kulkarni & Cheikhrouhou, 2024).

The ZTA application today is in highly secured ports and terminal logistics, where operations take place under a much more rigorous security regime due to their critical and sensitive nature. Ports form a major node within global logistics networks, and therefore, they cannot afford anything less than a world-class dimension of access-control complexity against unauthorized entry and against cyber threats. Such implementation of ZTA allows the deep knowledge of access in terms of a person's verified identity, security posture of the devices being used, and situational context on the ground at a given point in time, thereby significantly reducing potential incident occurrences at the logistics hub. (Kulkarni & Cheikhrouhou, 2024).

When we look to the future, ZTA's convergence with upcoming technologies such as AI (artificial intelligence) and digital twin technology creates tremendous improvements for intelligent access control in logistics. AI predictive analytics will draw heavily upon the secure data governance framework of ZTA in restricting access to critical analytical models and manifestation of sensitive operational insights. Digital twins, which are virtual representations of logistic processes occurring in real time, will require enforcement of stringent identity verification and access management to protect their integrity and reliable functionality. ZTA's diversity of authentication schemes will form an impregnable barrier allowing protection of the aforementioned advanced technologies from cyber threats and unwarranted meddling (Kulkarni & Cheikhrouhou, 2024).

2.6.5 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which became effective on May 25, 2018, is probably the most progressive and influential data protection legislation worldwide. It controls how organizations handle the personal information of individuals in the European Union (EU) regardless of the organization's own location. The core intention of GDPR is to give data subjects greater control over their own personal data and to align data protection law across the EU in order to assist the Digital Single Market (Li, Yu, & He, 2019). GDPR formalizes key principles such as lawfulness, fairness, and transparency, data minimization, limitation of storage, and integrity and confidentiality. It also entrenches several rights of the individual, including the right of access (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17), and the right to data portability (Art. 20) (Zaeem & Barber, 2020). Organizations are also required to incorporate "data protection by design and by default" into their technical and organizational measures (Art. 25), and to maintain detailed records of data processing operations (Art. 30). Despite diligent attempts at compliance, most organizations—especially those outside the EU—still find it difficult to comply with GDPR, the cause usually being non-transparency in privacy policies or poor technical controls (Zaeem & Barber, 2020). However, GDPR has initiated an international debate on data governance practices, which have influenced similar regulations in countries such as Brazil, India, and the United States, thus serving as an example of the so-called "Brussels Effect" (Mueck & Gaie, 2025).

In the next 5 to 10 years, the General Data Protection Regulation (GDPR) will continue to be a building block of data protection frameworks across the world but will encounter new challenges prompted by technological progress and growing digital ecosystems. Based on recent evaluations, companies continue to struggle with full compliance, particularly in terms of automated decision-making and the rights of data subjects, an indication that further guidance and possibly legislative amendments may be necessary for long-term effectiveness (Zaeem & Barber, 2020). As artificial intelligence and cross-border processing increase in sectors such as transport, logistics, and cloud computing, GDPR principles such as lawfulness, fairness, and accountability will need to be achieved in more complex technical ecosystems. This includes addressing current challenges with meaningful consent, processing immutable data structures such as blockchain systems, and transparency in algorithmic decision-making systems. As technological progress around the world continues, there is also increasing expectation that GDPR will serve as a model for other countries' regulations, further entrenching the EU's role in establishing global data governance norms (Li, Yu, & He, 2019). In this new environment, enforcement of GDPR in the future may increasingly rely on automated compliance mechanisms and regulatory technologies that enable constant monitoring of privacy practices across consolidated digital platforms.

2.6.6 Network and Information Security Directive 2 (NIS2)

The Network and Information Security Directive 2 (NIS2), also Directive (EU) 2022/2555, is the European Union's most recent legislative action to support increased cybersecurity within its Member States. NIS2 aims to supersede the original NIS Directive of 2016 and significantly increases the number of entities required to be in line with cybersecurity requirements, such as operators in critical sectors such as energy, transport, health, digital infrastructure, and public administration (Singh, 2023). The directive mandates robust cybersecurity risk management practices, supply chain security processes, and swift incident reporting within 24 hours of notification (Art. 23 NIS2). The directive also enforces a higher level of regulatory harmonization with the requirement to have each Member State adopt a full-fledged National Cybersecurity Strategy outlining policy priorities, resources allocation, and enforcement mechanisms (Mueck & Gaie, 2025). Furthermore, NIS2 strengthens enforcement capabilities by authorizing national authorities to impose severe fines and check compliance through inspection and audit. Another innovation of NIS2 is its focus on systemic digital resilience, not only internal but also outsourced and supply chain components. This is particularly relevant in the context of heightened interdependencies of digital ecosystems as well as arising cyber threats impacting multiple layers of infrastructure simultaneously. The directive further strengthens GDPR because a cybersecurity event impacting personal data would trigger requirements under both frameworks, thereby securing an integrated policy towards data protection and infrastructure security (Singh, 2023). Overall, NIS2 is a shift from reactive to proactive cybersecurity regulation in the EU's digital rulebook.

The role of the Network and Information Security Directive 2 (NIS2) in the next ten years will be to become further integrated into the operational environment of critical and essential service providers, particularly as digital infrastructures expand throughout the EU. NIS2, which replaces the original 2016 directive, introduces more rigorous tasks in risk management, incident reporting, and supply chain security that will be further embedded in logistics and intelligent transport systems (Mueck & Gaie, 2025). As the directive matures further, its focus will shift to ensuring cybersecurity resilience in more decentralized, data-centric, and automated environments. For instance, logistics platforms with vehicle tracking in real-time, predictive analytics, and Internet-of-Things (IoT) devices will face closer controls on monitoring system vulnerabilities, encryption, and cross-border coordination of incident responses. Member States have until October 2024 to deploy National Cybersecurity Strategies, but the directive's long-term effect will be when the strategies ripen into forward-thinking regulatory frameworks with live threat cooperation and automated surveillance (Mueck & Gaie, 2025).. In addition, the NIS2 directive also recognizes the developing threat environment and underscores the requirement for uniform cybersecurity baselines in the EU as well as operationalization of tools that can adjust to emerging modalities of cyberattacks against critical infrastructure. As highlighted by Singh (2023), the mainstreaming of NIS2 in national legal orders is a critical step towards an harmonized, strategic, and future-oriented cyber security approach that will become absolutely vital to protect the digital economy and foster trust in intelligent systems by the end of the decade.

2.6.7 JSON Web Signature (JWS)

JSON Web Signature (JWS) is a new standard for verifying data integrity and authenticity with JSON-encoded digital signatures. JWS, in the sense of the Internet Engineering Task Force (IETF) specification in RFC 7515, provides a mode of signing structure data with cryptographic algorithms like RSA, HMAC, or ECDSA in a compact, URL-safe encoding that is authenticatable and tamper-evident (Jones, Bradley, & Sakimura, 2015).

In the modern logistics era, JWS is increasingly applied to authenticate digital transmittals in Intelligent Access (IA) systems such as Transport Management Systems (TMS), Port Community Systems (PCS), and eFTI platforms. All these systems handle safe operating information vehicle credentials, route authorizations, emission classes that must be shared in a safe environment among a diverse set of stakeholders.JWS offers cryptographic assurance that the data has not been tampered with and comes from an authorized source (Jones et al., 2015).

For instance, when a delivery vehicle is attempting to enter a geofenced location, digitally signed access parameters like delivery window time or vehicle category can be verified by applying JWS. It assures real-time non-repudiation along with verification, both of which are heavily involved in IA application usage scenarios with autonomous decisions and must remain in conformity with regulation borders.Additionally, the compact form of JWS simplifies the integration with lightweight API protocols and HTTP headers, which are being used more and more in logistics IT infrastructures nowadays (Jones et al., 2015).

In the years to come, JWS will be at the forefront of progressively advanced and autonomous IA architectures. As logistics networks adopt Vehicle-to-Infrastructure (V2I) communications and decentralized control systems, JWS will offer the components for securely exchanging real-time compliance information between vehicles, infrastructure nodes, and cloud services. These signed messages could be access credentials, digitally bound emission declarations, or dynamic risk scores, all of which need cryptographic assurance to avoid manipulation or spoofing (Jones et al., 2015).

In addition, future use cases will see the convergence of JWS with digital twins, blockchain networks, and edge computing for facilitating localized verification of signed data without centralized trust anchors.This will be one of the critical considerations in delivering interoperability and security to distributed IA environments, with access control decisions made in real-time based on data packets that can be cryptographically validated. As logistics networks become more complex, JWS will remain a critical building block that delivers digital interaction that is secure, auditable, and adaptable to evolving requirements for governance (Jones et al., 2015).

3. Methodology

This chapter outlines the approach used to investigate the use of information standards, information systems, and information security in enabling Intelligent Access (IA) in road freight transport and port- and terminal logistics. The research aims to offer solutions to two pertinent questions: (1) what are today's and tomorrow's frameworks in enabling IA, and (2) how the frameworks influence IA performance such as efficiency, security, and regulatory compliance. In order to explore these objectives, qualitative methodology was employed alongside a systematic literature review and expert interviews. This dual methodology enables a thorough understanding of both the technological drivers behind IA and their operational and policy-level implications.

3.1 Data Collection

The data collection was conducted through two main sources: (1) a focused literature search to scan the existing literature on IA, and (2) eight expert semi-structured interviews to gather empirical data from transport digitalisation, logistics, and ITS practitioners. Through this multi-source data collection process, theoretical saturation is guaranteed and data reliability is increased through triangulation (Flick, 2014; Patton, 2015).

3.1.1. Literature Review

The data used for this research were gathered from a rich and organized strategy of gathering secondary as well as primary data in such a manner that they have provided rich, multi-dimensional, and profound insight into intelligent access (IA) within road freight and terminal-port port logistics. The core purpose of this process was to find information based on information standards, information systems, information security, and the sum of all of them for supporting intelligent access over freight transport networks.

Secondary data was obtained from a broad spectrum of academic journals, books, policy documents, technical reports, and industry publications. These sources were accessed through academic databases like Scopus, SpringerLink, ScienceDirect, and IEEE Xplore, making use of institutional access. Supplementary grey literature, such as EU directives (e.g., the eFTI Regulation), CEDR ISAC guidance, and white papers by the major logistics consultancies, added practical and policy-level background to the academic debate.

Systematic literature review was conducted to achieve transparency and replicability. This entailed the development of search strings from the fundamental themes of the research, screening documents for applicability, and the application of inclusion/exclusion criteria. Documents were considered for inclusion if they had explicit mention of digital transformation in logistics, especially by using interoperable systems, regulatory data standards, and cybersecurity mechanisms.

Besides desk research, qualitative primary data were gathered through expert interviews. The participants were professionals with experience in logistics systems, port operations, national road authority projects, and information security. The experts were purposefully chosen due to their direct experience in deploying or managing platforms like Port Community Systems (PCS), Truck Appointment Systems (TAS), Fleet Management Systems (FMS), and IT frameworks like Zero Trust Architecture (ZTA) and Amazon Web Services (AMS).

3.1.2. Expert Interviews

To complement the theoretical insights, eight semi-structured interviews were conducted with subject-matter experts across the logistics ecosystem. Participants were drawn from academia, logistics service providers, port technology developers, and national transport bodies. Experts were selected using purposive and snowball sampling techniques to ensure relevance and expertise (Bryman, 2016; Robinson, 2014).

Qualitative empirical data were gathered through semi-structured interviews with experts in road freight transport, port-terminal logistics, and intelligent access (IA) systems. Public authorities, private logistics service companies, and technology vendors engaged in digital logistics system implementation or analysis were represented.

A guide for the interview was prepared ensuring consistency in the interview but leaving room for probe questions. The schedule was created such that it would elicit both thesis research questions:

RQ1:What information standards, information systems and information security can be applied contemporarily and in the future for intelligent access in road freight transport and port- and terminal logistics?

RQ2:How can these contemporary and future planned information standards, information systems and information security affect intelligent access in road freight transport and port- and terminal logistics?

The interview schedule consisted of five broad categories:

Open-ended questions for the determination of background and relationship with IA

Utilizing today's standards and systems (such as eFTI, eCMR, RFID, TMS, TAS, GDPR)

Future technological trends and convergence in the field of IA (e.g., AI, IoT, machine learning, smart infrastructure).

Perceived impact on existing and future digital systems on IA performance metrics such as emissions, safety, and interoperability.

Final remarks, including ongoing projects, issues, and suggestions for other work in the future. The entire interview protocol used for the study is provided in Appendix A.This mixed-methods data collection approach combining theoretical constructs with practitioner experience enabled triangulation and improved the validity and richness of findings (Yin, 2018; Flick, 2014).

3.2. Data Analysis

Data analysis was carried out using a thematic approach, following the logic of Braun and Clarke's (2006) framework for qualitative data. Transcripts were coded and grouped according to the three core themes: Information Standards, Information Systems, and Information Security and two scenarios Contemporary(0-1 year) and future(5-10 years). These themes were directly mapped to the two research questions.

The final analysis words were:

Information Standards (e.g., eFTI, eCMR, RFID, EDI, Open Trip Model)

Information Systems (e.g., TMS, FMS, ERP, PCS, TAS, TOS)

Information Security (e.g., Zero Trust Architecture, JSON Web Signatures, GDPR, AWS)

These words were selected in order to capture literature relating to digital transformation of freight logistics, especially at the road-port interface.For content analysis, three analysis words were identified as the most important to define and categorize the data:

Information Standards – These standards include eFTI, eCMR, RFID, and EDI. These were utilized to determine how data standardization enables smooth communication and regulatory compliance among actors in freight logistics.

Information Systems – This was the category that encompassed the different digital platforms and mechanisms employed in managing logistic flows such as PCS, TMS, ERP, TAS, and FMS. The objective was to evaluate their contribution towards automation, interoperability, and real-time decision-making.

Information Security – Literature under this label included research or reports on cybersecurity models, GDPR compliance, encryption of data, Zero Trust Architecture, and safe cloud platforms such as AWS. These books were crucial in knowing how data integrity and confidentiality are maintained in digital logistics environments.

From the gathered literature, four analysis words were repeatedly employed as conceptual anchors for coding and theme development: information standards, information systems, information security, and intelligent access. These words were crucial not only for marking relevant data within texts but also for classifying emerging patterns and relationships in how these dimensions interact across different logistics environments.

The application of these particular terms was based on their salience in both grey and academic literature, which mirrored their place at the heart of digital transformation in logistics (Heilig & Voß, 2016). For example, "information security" came up regularly in debates around GDPR compliance, cybersecurity risk, and data protection in open API contexts, whereas "intelligent access" became an overarching concept that brought together booking systems, geofencing, and real-time data coordination.

To comparatively analyze how different information standards, systems, and security frameworks are constituents of Intelligent Access (IA), two structured tables were developed. One table allowed for cross-tabulation of the mentioned technologies from expert interviews and literature, and assisted in their ranking of significance in the near-term (0–1 year) and long-term (5–10 years) contexts. The two tables served complementary analytical purposes but had a consistent format structure.

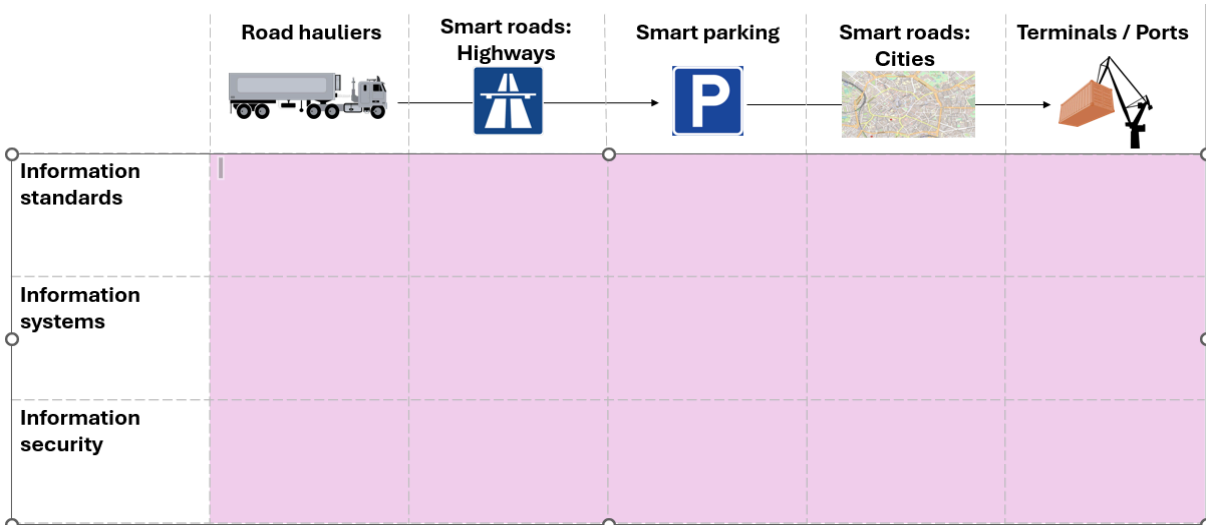


Table 1 Frameworks across logistics

Table 1: Positioning of Frameworks Across Logistics

The table has been drawn to visually represent the spatial and operating relevance of each of the frameworks to four main logistics markets:

Rows: The rows represent specific information standards, systems, and security frameworks drawn from literature and interview data. Examples include eFTI, eCMR, DATEX II, TMS, TAS, ZTA, GDPR, and blockchain.

Columns: The columns show the logistics application areas in which these frameworks are being adopted or are to be adopted. The following areas are involved:

Road Hauliers

Smart Roads (Highways and Cities)

Smart Parking

Terminals and Ports

All of the cells in the table were populated with either literature validation or expert judgment, where a specific framework is in fact being applied or would be reasonably likely to be applied in the future. Mapping in tabular format allows for analyzing the distribution of technologies among logistics infrastructure nodes.

Frameworks	Better use of existing infrastructure with traffic management based on time and place;	Less degradation of road infrastructure through improved management of weight, speed and routing of heavy vehicles;	Realizing climate objectives by reducing congestion and prioritizing climate-friendly vehicles, for example management of low emission zones, and this will give more transparent and greener logistics;	Increasing road safety through, for example, less overloading or improved insight into where safety incidents arise on the road network;	Creation of a level playing field between different haulers/carriers, improving compliance by haulers/carriers with regulations as set out by NRAs;	Improved control of the transport of abnormal loads and dangerous goods;	Controlled introduction of High Capacity Vehicles;	Faster and more unified and controlled processing of transport documents in cross-border transport through digitalization.
Information standards								
Information systems								
Information security								

Table 2: Intelligent Access Objectives

Table 2: Impact Relevance of Frameworks on IA Objectives

The second table was constructed to assess the functional relevance of the frameworks against eight identified Intelligent Access (IA) impact areas. These were drawn from ISAC documentation(CEDR ISAC, 2024) and IA goal expert consensus.

Rows: The same frameworks as in Table 1 (e.g., RFID, TMS, eFTI, AMS, etc.).

Columns: The columns symbolize the eight IA impact areas, i.e.:

Better use of infrastructure

Reduced road degradation

Contribution to climate objectives

Enhanced road safety

Reasonable compliance with hauliers

Improved management of abnormal/dangerous loads

Regulated use of High Capacity Vehicles (HCVs)

Streamlined cross-border digital documentation

All these cells in table 2 were also populated with literature and limited information from the experts. Both these tables were made for two scenarios: current(0-1 year) and future(5-10 years).

3.2.1 Expert Selection

Selection of participants was based on a combination of publication history, expert knowledge, professional role, and working on relevant projects. Snowball sampling was applied to select other

candidates through referral by early participants. Final selection ensured representation of the major sectors involved in IA, such as transport authorities, technology vendors, researchers, and logistics companies.

Interviewee backgrounds varied from researchers building IA-compliant systems (e.g., geofencing, TAS, and PCS) to policy experts on EU, freight data standardization, and port integration logistics. Having this vQualitative empirical data were gathered through semi-structured interviews with experts in road freight transport, port-terminal logistics, and intelligent access (IA) systems. Public authorities, private logistics service companies, and technology vendors engaged in digital logistics system implementation or analysis were represented.

4. Empirical Findings

Expert 1

Title: Logistics and digitalization Consultant

Contemporary Scenario(0-1 year)
Currently, IA is being tested out in modest yet significant ways. Some examples are real-time on-vehicle route adjustments, truck-priority at traffic lights utilizing smart systems, and managed access to terminals in a digital fashion through appointment-type systems. All these systems are vehicle- and trip-based information and tend to be supplemented with government-enforced restrictions such as emission zones, statutory weights, and time-variant access criteria. Yet all this is broken up into splintered fields. The insufficient infrastructure readiness, the lack of a harmonized system, and the limited digital translation of public policies considerably impede wider IA deployment. Furthermore, data exchange is frequently inconsistent, and digital standards such as e-CMR and Open Trip Model (OTM) are not uniformly implemented, resulting in operational silos.

Future Scenario (5–10 years)
In the near future, IA will play a pioneering role in enabling fully data-driven, automated, and dynamic access control. Pre-approved credential-enabled vehicles will be provided with comfort in terms of seamless cross-border access conformity, routing preference based on policy, and constant access to low-emission zones or terminals.
Advanced Vehicle-to-Infrastructure (V2I) communication systems will enable real-time access decision-making, and AI-informed products will support routing management, compliance checking, and congestion relief. Such transformation will, however, depend on the adoption of harmonized standards like eFTI and secure integration of public and private systems. One digital ecosystem, underpinned by strong cybersecurity practice and regulatory convergence, will be key to scaling IA in a trustworthy and interoperable manner.

RQ1

1. Information Standards
Interviewee spotted many current and emerging information standards relevant to making Intelligent Access happen for both road freight transport and terminal logistics. These standards allow interoperability between government systems, logistics providers, and infrastructure services.

Contemporary Scenario(0-1 year)
Datex II is a European traffic data standard based on XML for real-time exchange of infrastructure and condition data.Open Trip Model (OTM) is the Rules for digital communication of vehicle characteristics, routing, and access entitlements (e.g.: legal weight, emission class, dimensions).
e-CMR is the Digital consignment note standard used at limited operational frameworks (~5% adoption), in principle paving the way for the digitization of global logistics. Fleet and Transport Data Protocol can be regarded as proprietary, but on a case-by-case basis conforming to industry formats for route planning, GPS tracking, and compliance reporting.

Future Scenario (5–10 years)
EFTI (Electronic Freight Transport Information): Intended to support digital data sharing between logistics operators and enforcement authorities. It is not deployed on a large scale yet but will be paramount to the future IA.

Challenges raised are Lack of unified adoption in different sectors,Inconsistent standards from one EU country to another and Very strong reliance on all the stakeholders adopting the same digital language.

2. Information Systems
Contemporary Scenario(0-1 year)
Fleet Management Systems (FMS) is installed in the vehicles; collects and transmits real-time data on location, speed, dimensions, and compliance status.Transport Management Systems (TMS) is the office-based system used for dispatch planning, route optimization, and administrative control.Port Community Systems (PCS) is used in port logistics to manage container readiness and truck access coordination.

Future Scenario (5–10 years)
Integrate seamlessly municipal traffic control and private logistics.Vehicle-Infrastructure (V2I) communications for immediate decision-making.AI trip planning against regulatory constraints

Interoperability and data integration in these systems remain serious barriers.Market fragmentation caused confusion up to 20 different system providers maximally exist in the Netherlands each having a different scope and setting of standards.

3. Information Security / Data Security
Interviewee didn't know much about the enactment in cybersecurity, but set forth a perspective on data security: the more systems interact in real time, especially across borders or by third-party vendors, the added risk multiplies.
Preventing the impending threat: General common cyber security standards will be accepted; encryption, doorway monitoring, and restrictions on data hosting concerning IA operations so that it may be considered ethical and be trusted.

RQ2

1. Information Standards
Standards that enable IA to perform robustly and at a scale. These include such existing data standards such as Datex II (for most traffic data), Open Trip Model (OTM) (for trip and vehicle metadata), and e-CMR (for digital freight documentation) as being presently applied in disparate forms but could be much more efficient if universally applied.

Contemporary Scenario(0-1 year)
These permit limited functions of IA such as identification of vehicles electronically and monitoring of routes. Yet these standards are seen to be taking off only in an irregular manner in the European Union and among logistics actors.

Future Scenario (5–10 years)
Once introduced, eFTI will make authorities digitally access verified freight data transforming regulation discharge and access permissioning.

2. Information Systems
The interconnected digital systems included the Fleet Management Systems (FMS), Transport Management Systems (TMS), Terminal Appointment Systems, and so on, really do form the operational backbone for Intelligent Access.
Operational Impact on IA Implementation:

Contemporary Scenario(0-1 year)
These systems already collect and relay important data pertaining to vehicle weight, emissions category, and position-all relevant to the IA policies.

Future Scenario (5–10 years)
In the near future, these will be advanced Vehicle-to-Infrastructure (V2I) systems specifically enabling automated routing decisions based on real-time infrastructure constraints and environmental rules.

System Integration Challenge: Tight coupling between the private systems (FMS/TMS) and the public infrastructure (traffic lights, gates) is core to the IA setup, and thus integration, interoperability, and unified data models are paramount for an impact.

3. Information Security / Data Security
As the vulnerabilities of IA systems scale up, data security becomes not just an issue of technicality but an essential element to the very credibility and functionality of IA itself.

Contemporary Scenario(0-1 year)
A number of associated facilities (e.g., solar system, logistics apps) are managed on remote servers, often outside the EU, resulting in dependencies and possible vulnerabilities.
Mishaps through unauthorized access to centralized traffic control systems or logistics networks may cause systemic disruptions for example, paralyzing traffic by altering access rules or by disabling smart lights.No visibility on where or in what manner the data gets stored or transmitted.

Future Scenario (5–10 years)
Standardized protocols in cybersecurity for the logistics and transport infrastructures. Strong encryption and access control of sensitive data (e.g., vehicle identity, route plans). Regulatory oversight in data-hosting and sovereignty. Risk assessments before adopting new systems or expanding the digital IA infrastructure.

Expert 2

Title: Advisor of Urban Logistics, Intelligent access and Digital transport infrastructure

Contemporary Scenario:
Intelligent Access (IA) is still a theoretical model and not yet a complete implemented system. Its goal is to facilitate flexible and data-driven regulation of freight vehicle movement in logistics and urban environments. Currently, real-world implementation is very low, with only early experiments being carried out in a few nations. Current systems do not have the flexibility to provide the type of adaptations that IA would need, e.g., modulating access according to local events, noise areas, or time-based restrictions. The digital infrastructure required to support IA—such as interoperable platforms, standardized operation data, and secure communication channels—is missing in large part,

particularly for small and medium-sized logistics providers who tend to use manual coordination and ad hoc channels such as messaging apps. Consequently, IA is hindered in terms of enforcement and operational viability with the existing setup.

Future Scenario (5–10 years)
In the future, IA is seen to operate as a negotiated, context-aware system where access decisions are dynamically taken from real-time information like vehicle weight, emissions class, delivery schedules, and local regulatory constraints. Instead of fixed rules, access would be controlled by systems that enable real-time negotiation between transport operators and infrastructure authorities. This will be underpinned by new standards and technologies, such as digitally signed access statements, event-driven planning systems, and secure communications protocols. The success of these systems will rest on their capacity to be low-cost, scalable, and interoperable, most importantly to support adoption by smaller stakeholders. Future IA is likely to reconcile strict regulatory compliance with operational flexibility, and hence will be a central enabler of smart and sustainable logistics.

RQ1

1. Information Standards
Contemporary Scenario(0-1 year)
Currently some operational standards trip-oriented like Open Trip Model (OTM) are being adopted to facilitate award-winning solutions, real-time decision-making, route optimization, and adaptive access permissions. They have proven useful, even at this initial stage, in pilot applications and early stages of digital freight projects. Additionally, geofencing is also being used in some urban logistics settings to provide on-the-spot enforcement of access regulations and webhook-type updates allow a more agile event tracking and coordination.

Future Scenario (5–10 years)
In the future, Logistics Event Ontologies aim at standardizing event semantics in the area of freight and logistics to provide cross-system interoperability and situational awareness. Also emerging are JSON Web Signatures (JWS), which provide an elemental mechanism for trusted and verifiable data exchange between logistics operators and authorities. These standards thus decrease dependency on expensive and complicated API infrastructures, making them especially relevant to small and medium-sized enterprises (SMEs). Consequently, these standards under development will ensure that Intelligent Access systems evolve to become more secure, scalable, and inclusive for gradual yet pragmatic acceptance grounded in real-world logistics operations.

2.Information Systems
Contemporary Scenario(0-1 year)
Port Community Systems applied in advanced ports are centralized platforms allowing integration of access control, cargo tracking, and stakeholder interaction.
Endpoints and EDIs are relatively widely spread across the industry, albeit considered for now as rather outdated since they have insufficient flexibility or interoperability.ERP, TMS, and WMS are not widely adopted by small and medium logistics firms mostly due to high implementation costs and IT complexity.

Future Scenario (5–10 years)
Event-driven systems allow for sharing and constant update of information so that all stakeholders can respond dynamically to changing conditions.

Standardized APIs and secure messaging (e.g., Webhooks) would enable seamless and secure communication between systems.
Integration with smart planning systems, potentially with support from AI and machine learning, to provide automated suggestions for routes, scheduling of allotments, and analysis of traffic pattern on live information.

3.Information Security
Contemporary Scenario(0-1 year)
Currently, information security in Intelligent Access (IA) mostly depends on basic tools such as secure APIs and limited RFID use, typically used by larger logistics firms. However, many SMEs are not protected well enough.

Future Scenario (5–10 years)
Anticipated future JWSs or JSON Web Signatures are now hailed as the new magic potion for secure verifiable data exchange that lessens the pains in developing complex APIs. Webhooks serve real-time secure updates, while geofencing permits localized access control. Heightening cyber threats, especially those modelled as state actors, face future IA architectures to low exposure compartmentalized models for a scalable secure implementation across the logistics industry.

RQ2

1. Information Standard
Contemporary Scenario(0-1 year)
Presently, Open Trip Models, which are probably some of the many travel type operating standards being adapted, allow dynamic decision-making, real-time route optimization, and adaptable access permissions. This already shows a value in pilot projects and early-cyclical digital freight. In addition, geofencing applies in certain urban logistics environments to foster local enforcement of access rules while event tracking and coordination becomes rich in real time facilitated by webhook-based updates.

Future Scenario (5–10 years)
Moving toward the future, Logistics Event Ontologies will make a step toward a common semantic event in freight and logistics, allowing systems to interoperate and be situationally aware of one another. Also coming up are JSON Web Signatures (JWS), another major actor in establishing a trusted and verifiable data exchange between operators and authorities in logistics. The standards will enable an SME economic implication by reducing infrastructure cost and complexity on APIs, while the development trend promises a standardization of Intelligent Access systems that are more secure, climbed, and inclusive for practical little-by-little adoption as per real operations in logistics.

2.Information systems
Contemporary Scenario(0-1 year)
The large logistics usable interface such as PCS serves the large central coordination and real-time access control functions to support effective operations while small freight operators are digital illiterate and cannot really participate in IA, resulting in a widening digital gap in the industry.

Future Scenario (5–10 years)
Event-driven architectures, standardized APIs, and secure messaging protocols (such as webhooks), will be used for real-time coordination in IA systems in the coming years. The integration of artificial

intelligence will streamline planning and decision-making. In order for the bulk of adopters-in particular SMEs-to embrace them, future systems will need to be priced affordably, be scalable, and lend themselves easily to integration; thus enabling an inclusive and efficacious implementation of IA.

3. Information security

Contemporary Scenario(0-1 year)

Information security presently constitutes the most salient vulnerability in the implementation of Intelligent Access (IA), especially critical among small and medium logistics firms from the low level of IT maturity. Equality in security protocols is not among larger ports and transport hubs, and most of the case happens to be that of small and medium enterprises; they have an older system with very few walls that make them vulnerable to breaches and data misuse. This lack of common security creates gaps in trust and reliability towards the advantages of using IA-specific systems.

Future Scenario (5–10 years)

Future IA systems will largely depend on more robust, scalable security architectures through JWS for verifiable, tamper-proof communication together with event-driven tools such as webhooks for secure data exchange. Moreover, IA systems must be compartmentalized, with low exposure architectures to achieve resilience against potentially severe cyber threats, especially state-sponsored attacks. Privacy including authentication and data integrity will be very important characteristics to be built into future IA systems that should safely scale in all freight and port logistics sectors.

Expert 3

Title: Senior Researcher of Digitalization and Transportation

Contemporary Scenario(0-1 year)

In the present situation, Intelligent Access (IA) remains largely in the pilot and planning phase, particularly in Sweden, and is mainly used on "abnormal transports" like oversized or overweight trucks. The primary application of IA currently is conditional access to road infrastructure depending on vehicle conformity to certain criteria, for example, weight, speed, or emissions. Real-life applications being tested include geofencing to control speed on bridges and access to environmental zones by vehicles. But existing implementation is patchy and relies much on manual means, like Sweden's TRIX permit system, with no integration of real-time data or automation. The most significant impediments to widespread IA implementation are limited availability of detailed infrastructure data and non-harmonized digital standards across areas.

Future Scenario (5–10 years)

In the future, IA will develop into a more advanced and integrated system that facilitates dynamic, automated access decisions in both road and terminal settings. This will comprise real-time car compliance checks using geofencing, AI-routing, and telematics. Pilots like Oslo's and Volvo's fleets are pioneering the way by testing smart city networks with the capability to manage car behavior electronically. Full interoperability and cross-border application, however, require quality data governance, improved digital infrastructure, and standards such as EFTI and ISO models aligned. In this future vision, IA could transform the logistics sector by enabling policy-based routing, seamless coordination among transport stakeholders, and better regulation of freight flows—if the underlying systems are secure, data-rich, and privacy-compliant.

RQ1

1. Information Standards

Contemporary Scenario(0-1 year)

Information standards such as TRIX in Sweden and other national regulatory frameworks that govern the abnormal and heavy freight transports take place with set process narratives. The systems allow the authorities to assign access permissions; however, they are highly manual and not standardized across countries. Some logistics companies employ routing systems that could provide the access management function, but it's not done purposefully for Intelligent Access.

Future Scenario (5–10 years)

Future implementations of eFTI and ISO Intelligent Access framework standards ought to lead to more automated cross-border access control. Real-time sharing of data regarding freight vehicles, infrastructure, and authorities will now be made possible. Collaborative means like the CEDR framework will aspire to achieve Europe-wide rules for smarter and safer logistics on roads and terminals.

2.Information systems

Contemporary Scenario(0-1 year)

As of now, fleet management and routing systems constructed by organizations like DHL are used to support access constraints for route planning. While these systems offer a certain level of control, it is often manual and not totally integrated with infrastructure data.

Future Scenario (5–10 years)

Ways to move forward include automated geofencing systems, smart infrastructure platforms, and real-time digital permit systems for dynamic location-based access control. Vehicles will automatically adjust speed or route when infrastructure conditions change so as to achieve better safety, compliance, and traffic efficiency in road freight and port logistics.

3. Information security

Contemporary Scenario(0-1 year)

The present framework for safeguarding information in road freight and port-terminal logistics rests upon regulations such as GDPR, which assure privacy and responsible usage of personal data and transport-related data within Europe. Security concerns are further simplified by employing basic cloud protection mechanisms, such as secure configuration on platforms like AWS, which are generally used to store and manage logistics data. However, most of the systems still rely on manual access mechanisms and have few cybersecurity layers in permit systems and infrastructure databases, exposing themselves to unauthorized access and inefficiencies.

Future Scenario (5–10 years)

In the future, information security will adopt mechanisms that facilitate advanced and automated Intelligent Access systems. On the basis of Zero Trust Architecture (ZTA), these systems will enforce strict verification of each user, device, and system component before access is granted, thus enhancing trust and control exponentially. Real-time intrusion detection systems will assess vehicle networks and critical infrastructure in search of threats, while secured telematics and IoT integration will protect all data flows between vehicles, smart roads, and terminal systems. This leap forward will be instrumental in achieving safe, scalable, and fully digital Intelligent Access operations.

RQ2

1. Information Standards

Contemporary Scenario(0-1 year)

Testing is still under the use of national standards like TRIX and routing systems that enable the implementation of basic Intelligent Access by controlling where and when special freight vehicles may travel. Unfortunately, since such IA enforcement systems are mostly manual and vary from country to country, the possibility of automated and consistent IA enforcement is very much limited.

Future Scenario (5–10 years)

Going forward, such standards as EFTI and the ISO IA frameworks will enable real-time data exchange with digital permits and make IA much more automated, efficient, and scalable. Such enhancements will also allow the authorities and logistics operators to ensure that only compliant vehicles access sensitive roads or terminals, thereby enhancing safety, efficiency, and environmental performance.

2.Information systems

Contemporary Scenario(0-1 year)

Intelligent Access is affected by information systems that allow for a more intelligent and controlled utilization of road and terminal infrastructure. Typically, permit management systems or routing software should assist in simple access decisions. However, their effectiveness is limited since they require manual processes that rely on disparate data.

Future Scenario (5–10 years)

Future systems will extend the concept of Intelligent Access by being data-driven, automated, and using geofencing. This means that the systems will be automatically checking whether a vehicle adheres to the requirements or otherwise manages access based on time or location, improving safety, reducing wear and tear on roads, and facilitating smooth logistics activities.

3. Information security

Contemporary Scenario(0-1 year)

Security measures nowadays currently protect both personal and operational data and provide compliance and privacy. But at the same time, it restricts sharing and automation, making it difficult to realize real-time IA solutions. Lack of modern, advanced, system-wide security raises the threat of data breaches or unauthorized access.

Future Scenario (5–10 years)

Future frameworks on security will conduct secure, real-time communication and decision-making in AI systems. It will prevent unauthorized tampering and allow the entry of only authorized vehicles and users into restricted areas. Furthermore, they will also help build trust among digital access controls. Strong security will also remain imperative for scaling IA across borders and systems while ensuring safety and compliance.

Expert 4

Title: Chief Engineer at Institute of Maritime Logistics

Contemporary Scenario(0-1 year)
In the current scenario, Intelligent Access (IA) is largely carried out by Truck Appointment Systems (TAS), especially in major ports such as Hamburg. TAS helps in controlling truck traffic, avoiding delays, and coordinating terminal capacity with vehicle arrival times, giving efficiency to the operation. Nevertheless, issues of appointment no-show and terminal operator monopoly over access control persist. There is very much a strong demand for greater collaborative and open access models reflecting the interests of the smaller operators in logistics.

Future Scenario (5–10 years)
In the future, IA will be more integrated and adaptive. It will certainly include AI-driven predictive analytics and enable initiatives on sustainability, like coordinating access windows with charging hours for electric trucks. The future vision also encompasses integrating IA systems with wider platforms such as TOS (Terminal Operating Systems) and PCS (Port Community Systems), particularly in low-resource or minor terminals, to provide equitable and inclusive access throughout the logistics network. This future revolution is dependent upon modular intelligent systems that can exchange data in a seamless manner, predict planning, and community-based governance.

RQ1

1. Information Standards
Contemporary Scenario(0-1 year)
Currently, the essential information standards include RFID (Radio Frequency Identification) for tracking and identification and eCMR (the electronic consignment note) for digital freight documentation. These are standards that allow the office to digitally exchange logistics data with each other, which are applied in varying degrees of use, usually according to company size and infrastructure. Port Community System (PCS) and other digital platforms depend on these standards for interoperability with all transport actors.

Future Scenario (5–10 years)
In the future, it is believed that such information standards will develop towards more interoperability, real-time data exchange, and a multimodal approach toward integration. New emerging concepts, such as blockchain-based standards, could provide secure and transparent tracking of freight activities. Provisions to expand existing standards for autonomous systems, electric freight vehicles, and cross-border logistics operations are in progress.

2.Information system
Contemporary Scenario(0-1 year)
Currently, the principal information systems supporting logistics operations are Transport Management Systems (TMS) for the planning/execution of freight movements, Fleet Management Systems (FMS) for monitoring vehicle operations, Port Community Systems (PCS) for coordinating port stakeholders, Terminal Operating Systems (TOS) for managing container handling in terminals, and Truck Appointment Systems (TAS) for scheduling/regulating truck arrivals in terminals. These systems have either been established independently or exist simply as a base of partial integration based on the sheer size and level of digital maturity of the logistic system.

Future Scenario (5–10 years)
In the future, information systems will become more intelligent, integrated, and data-driven, optimizing logistics networks' efficiency and responsiveness. Among the critical advancements will be AI-assisted platforms for predictive scheduling and anomaly detection, IoT-enabled systems that will provide real-time tracking and automated access verification, cloud-based infrastructures for seamless data sharing between stakeholders, and modular and scalable TOS/TAS platforms to cater for small and infrastructure-poor terminals. These proposed systems will support collaboration and dynamic adaptation to real-time operational changes, greatly advancing the implementation and impact of Intelligent Access (IA) in road freight and port terminal logistics.

3.Information Security
Contemporary Scenario(0-1 year)
At this time, road freight information security and port terminal logistics concentrated on data privacy compliance and the regulation therein, notably the General Data Protection Regulation (GDPR). Emphasis is placed on secure data exchanges among key systems such as Truck Appointment Systems (TAS), Port Community Systems (PCS), and Terminal Operating Systems (TOS) for the purposes of operational continuity and trust among stakeholders. Access control measures are being instituted to safeguard against unauthorized entry and subsequent use of systems so that sensitive operational data can remain protected. Further, many organizations are now using cloud services, such as AWS, hosted and configured with strict security protocols for the management of logistics data. Also, monitoring tools like surveillance cameras and RFID tags are being employed that require secure data storage and transmission methods to avert breaches or misuse.

Future Scenario (5–10 years)
Information security in road freight and port terminal logistics will evolve in the future into complex forms of intelligent integration to easily support the increasingly complicated plans for Intelligent Access. Key in this is a Zero Trust Architecture, which allows continuous authentication of any device, user, or application regarding access to anything essential to a system. Real-time AI-enabled threat detection and response would analyze trends of behavior patterns to detect and mitigate security risks. Increased use of sensors and connected devices makes it vital to have encrypted IoT communication: to secure the integrity of data while in transmission. Ethical and explainable AI governance will also define how algorithms make access decisions. Lastly, automated compliance monitoring will help logistics operators comply with changing data protection laws, allowing secure handling of the information within the digital domain and lawfulness on all counts.

RQ2

1.Information Standard
Contemporary Scenario(0-1 year)
At the moment, the information standards provide a basic level of interoperability and visibility for data, which are prerequisites for IA implementation. Terminals and freight operators can, therefore, share standardized data for scheduling and access control with each other. Unfortunately, uneven adoption practices and technical limitations, such as RFID interference hurdles in metal-dense environments, have, thus, hindered a full-scale integration approach. Nevertheless, they are the backbone of coordinated access and tracking in consultation with the present IA systems.

Future Scenario (5–10 years)
A more advanced and harmonized standard will lead to greater automation, predictability, and scalability for IA. The seamless data exchange across transport modes and digital platforms enables enhanced decisions and dynamic access control. As one set of standards becomes adopted by an increasing number of ports and logistics networks, IA will transition from being a series of isolated, terminal-specific systems to a collaborative, ecosystem-wide framework that brings efficiencies, security, and agility for the entire supply chain.

2.Information system
Contemporary Scenario(0-1 year)
Access to modern information systems is structured, predictable, and controlled within the logistics facility, thereby enhancing coordination and reducing delays. Planning of flows, managing terminal capacity and access to the gate at the right time are some of the contributions made through these systems. Limited integration and lack of real-time data sharing between systems can restrict the full potential of IA, especially when it comes to small or less digitized terminals.

Future Scenario (5–10 years)
The next generation of systems will make IA more proactive, automated, and integrative. Real-time data sharing and predictive analytics are expected to improve access planning, decrease congestion, and enhance resource utilization. Scalable solutions will make effective IA implementation, even for small terminals, making intelligent access even more pervasive and effective across the logistics ecosystem.

3.Information security
Contemporary Scenario(0-1 year)
In Intelligent Access, confidence, reliability, and stability hinge on strong information security. Stakeholders may be reluctant to share data without it, disrupting the seamless coordination that IA relies upon. Data breaches or insecure systems could lead to delays in operations, unauthorized access to ports, and loss of service continuity, all the more so at busy terminals.

Future Scenario (5–10 years)
Future security frameworks will facilitate IA systems that scale, automate, and are resilient. With IA, operating in a more predictive and autonomous way (self-scheduling trucks, for example, or AI-controlled terminal access), security of a high order will ensure that these systems remain immune to cyberattacks and manipulation, so as to foster the confidence of all stakeholders. Advanced security will foster further integration and data sharing across platforms, which will boost the direct operational and adaptive efficiency of logistics operations.

Expert 5

Title: Postdoctoral Researcher at the Integrated Transport Research Lab (ITRL)

Contemporary Scenario(0-1 year)
Intelligent Access (IA) is still in its nascent phase, with deployments mostly confined to small-scale pilots. Geofencing is currently the underlying building block, supporting access control based on pre-defined spatial and safety criteria like icy roads, environmental zones, or construction sites. This system, though not yet intelligent, represents a rudimentary type of regulated access, assisting authorities and operators in enforcing basic safety and compliance regulations in logistics corridors.

Future Scenario (5–10 years)
In the coming years, IA will become an even more intelligent and dynamic platform.This includes application of real-time data, online permit applications that can be automated, and in-car systems that display accepted routes and access permissions. Artificial intelligence and the Internet of Things will facilitate real-time decision-making, with the capability to modify routes based on traffic, infrastructure capacity, and regulatory limitations. In addition, surveillance systems and vehicle-infrastructure communication devices will enforce and check compliance automatically. Although promising, the shift to such systems is expected to be resisted due to issues such as low driver compliance, high technology investment, and reluctance by logistics companies unsure of financial payback. Thus, the success of IA also depends not just on technical innovation but on harmonizing human behavior and institutional collaboration with digital capabilities.

RQ1

1. Information Standards
Contemporary Scenario(0-1 year)
RFID is used to track vehicles and their loads, providing information on where transport units are at any point in time and how they move.eCMR (Electronic Consignment Note) and eFTI (Electronic Freight Transport Information) are good standards but they are not so far incorporated into current Intelligent Access (IA) systems.

Future Scenario (5–10 years)
eCMR (Electronic Consignment Note) is a digital version of the consignment note that serves to harmonize documentation associated with the movement of freight.eFTI (Electronic Freight Transport Information) is a European regulatory framework aimed at establishing the common standardization of data on freight transport to be exchanged between operators and authorities.Common data sharing platforms are envisioned as the standardized environments in which municipalities, OEMs, logistics providers, and authorities will operate with the use of standardized protocols.

2. Information Systems
Contemporary Scenario(0-1 year)
Intelligent Access has the top ranking at present when compared to other systems such as Geofencing, if used to describe vehicle access limitation and assistance to designated places such as icy roads or environmentally sensitive areas. Other system descriptions were mostly scanty, given that fleet management systems and transport management systems formed part of the existing logistics ecosystem, into which these were integrated into operational processes. It was common in manual permitting systems that they were slow and cumbersome, making them impractical for most logistics firms. This situation has seen the noncompliance of most players regarding access rules.

Future Scenario (5–10 years)
Future developments include the transition of the permit application process into the digital environment, allowing traffic operators to apply for access through digital channels. Approvals would then be potentially visible in real-time in vehicles. Future developments might also include in-vehicle displays announcing status of permissions or restrictions for access, especially during surveillance or inspections. There is further potential for artificial intelligence to be integrated into Intelligent Access systems, where on-the-road messages would alert drivers ahead of time of restricted roads, weighing stations, or permits to access information regarding the applications required. Intelligent Access is

considered to be a tool with which authorities such as Trafikverket will monitor wear and tear on the roads and the extent to which proactive maintenance can be planned.

3.Information security

Contemporary Scenario(0-1 year)

The contemporary information security practices concerning road transport and port-terminal logistics have more shortcomings, which tend to limit the successful adoption of the Intelligent Access (IA). One of the critical factors is that of implemented formality in terms of data security protocols, since existing logistics systems almost always lack solid, standard compliance with data sharing across platforms. This made logistics companies reluctant in sharing operation data because of the risk of misuse, competitive sensitivity, and sometimes vague compliance demands. There are also no clear rules on the ownership of the data and how they will be protected. Most of the concerns raised by this withholding of data relate to confusion in the area of regulations and access permissions, which should also not define what data could be shared. In addition to this, privacy regulations—like those accompanying the GDPR—are related greatly to sensitive information like identities of the drivers and the contents of cargo but incorporation hasn't yet been done well into the operational systems.

Future Scenario (5–10 years)

In the future though, IA systems will adopt secure digital communication techniques like self -end-to-end encrypted networks and digital access-authorizing models that guarantee safe data sharing among stakeholder users. One good strategy is to align with Zero Trust Architecture (ZTA), a security model in which data access from all users and systems is continuously verified before it is granted access to the data, thus minimizing security breaches. Also, another trend of consideration holds through cloud-based security, like those being offered by AWS, for secure data storage and scales sharing in integrated logistics networks. The future will also call for more enhanced privacy and data sharing contracts with legally and operationally defined protocols for access rights, ownership and accountability thus ensuring trust, transparency, and compliance in the Intelligent Access ecosystem.

RQ2

1. Information Standards

Contemporary Scenario(0-1 year)

RFID technology allows for basic access control based on location whereby it radically provides monitoring of vehicles entering restricted or sensitive areas.Missing digital and standardized data formats such as eCMR and eFTI hampers the automation of access-control decisions and their verifications against compliance, resulting in scattered but reliable information across stakeholders. Under the absence of standardization, IA systems are entirely disintegrated, precipitating manual processes and agitated inefficiencies that clinch compliance and run down the trust of systems.

Future Scenario (5–10 years)

Verifies real-time transport documents along with cargo and route information in support of dynamic, data-dependent accessibility decisions.Digitalizes the permission channel through which approvals can take place under an integrated environment with no delay due to human engagements, propelling the quality accuracy of enforcement.Enhances interoperability of the systems through consistent and efficient communication across various logistics and government platforms.Builds trust amongst stakeholders, thus eliciting adoption of IA by ensuring that all actors operate under clear common rules and protocols.

2. Information Systems

Contemporary Scenario(0-1 year)

The current systems are entitled as the key layer of automated identification of vehicles within the frameworks of Intelligent Access. The systems do possess a feature of automatically recognizing if an approaching vehicle is entering the restricted area; hence, it issues either a warning or denial of access. The systems further facilitate the movement of vehicles and could be put in interaction with Intelligent Access operations when data on vehicle weight or payload type are made available. However, any limitations introduced into the system-slow, manual permit processes, in particular-will diminish the capacity of Intelligent Access. As a consequence, many trucks move into restricted areas with no permits due to long processing delays that fuel noncompliance.

Future Scenario (5–10 years)

By having state-of-the-art digital platforms facilitate real-time access grant decision-making, the throughput of work will be increased, violations will be decreased, and compliance with Intelligent Access will be made more imminent as expected for the coming systems. This shall also strengthen enforcement by providing immediate, readily available access records to validate and back-track access granted during transit. Enlightenment and anticipatory user-centric approach are expected from the applications of AI into Intelligent Access systems in terms of preferred route setting and adherence to their restrictions. In addition, the relationship between road condition data and access permits will allow real-time tweaks to protect sensitive road segments from turning into dust with heavy vehicle traffic.

3.Information security

Contemporary Scenario(0-1 year)

It is currently considered that the absence of any robust form of information security has a debilitating effect on the adoption of Intelligent Access (IA) technology and its actual use in road and port-terminal logistics. The absence of secure data protocols undermines trust in the IA system itself, since logistics providers are very reluctant to share sensitive information that would actually contribute to participation and system adoption. This reluctance leads to limited data sharing and poor interoperability, resulting in disjointed environments where IA can do little to make informed and real-time access decisions. Besides, compliance risks only rise with unestablished data ownership and enforcement mechanisms, thus creating potential pathways for violations in privacy—GDPR being one legal framework that can get triggered here. Such a state and lack of consistency create further disincentives for investment from the stakeholders who would be the OEMs and technology providers, who are unlikely to support or develop IA-enabling technologies in the absence of data quality and protection assurances.

Future Scenario (5–10 years)

Conversely, it is anticipated that upcoming advancements in information security will enhance stakeholder trust with reliable and widely accepted protocols, including those aimed at protecting data and calling for active participation. This, in turn, will facilitate real-time and secure decision-making enabling IA systems to process and promptly respond to vehicle location, cargo type, and permits. Besides, the clarity provided by defined protocols will make accountability and liability a well-established aspect, which is crucial in the situation of AI-assisted systems where determining who bears responsibility for any mistakes becomes of paramount importance. In conclusion, keeping up with legal standards, such as GDPR, will allow comprehensive monitoring as well as ensuring the

protection of personal data and operational data, especially during confinement scenarios, further enhancing the integrity and scalability of Intelligent Access.

Expert 6

Title: Researcher at TalTech and Expert at the Digital Logistics Centre of Excellence (DLCE)

Contemporary Scenario(0-1 year)
In the present situation, Intelligent Access (IA) remains in its infancy of implementation, hampered by fragmented systems, uneven data flows, and low digital maturity. It is envisioned as a real-time, digital, non-intrusive access control and compliance verification mechanism for road freight and terminal logistics. Current systems are based on a mix of transport documentation, vehicle and driver information, and records of logistics activity, but much of this is still manually processed or weakly integrated. IA is currently plagued by bottlenecks caused by poor standardization, systemic interoperability gaps, and nascent but underdeployed technologies such as eFTI and eCMR.

Future Scenario (5–10 years)
IA in the future will be an active, automated system based on harmonized data exchange and real-time system integration. It will be supported by technologies like smart tachographs, 5G networks, AI-based validation algorithms, and secure telematics. IA frameworks will shift towards enabling seamless digital enforcement of access rights through intelligent system coordination, reducing the requirement for physical inspections and manual interventions The coming of age of information standards such as eFTI and the use of semi-centralized, interoperable data models—likely regulated by the EU or UN—will be instrumental in supporting cross-border, multimodal IA systems. Security will also be a foundation stone, with zero-trust architecture, authenticated queries on data, and encrypted access logs making IA reliable, scalable, and trustworthy in ever more complicated digital logistics contexts.

RQ1

1. Information Standards
Contemporary Scenario(0-1 year)
Interviewee cited a number of existing information standards in the interview, although with varying levels of adoption and maturity:eCMR (Electronic Consignment Note) is currently in usage but not fully operable or consistently embraced. Individual implementations exist, yet harmonization among EU members states still lacks.Electronic Data Interchange(EDI) is still widely adopted for the exchange of data using systems, simple but totally functional.Radio Frequency Identification(RFID) is applied in certain cases for tracking and verification, but there is no formal standardization.The mode-specific standards (like SMGS for the rail) is mentioned relevant to multimodal contexts, but not the main focus for the integration of a road-port.IMO standards and bill of lading (for ports) are being now used to manage the documentation of maritime transportation and delivery processes.

Future Scenario (5–10 years)
According to the interviewee, however, a lot of work is taking place toward standardization of data for digital logistics and IA.eFTI (Electronic Freight Transport Information)is the Formalization through EU delegated acts and aims to provide structured datasets for consignment and transport movement data.FT datasets define every transport "leg" so that data could be validated step by step. Proposed within the EU as a semi-centralized data model. With that, there will be harmonized, free-to-use

standards across modes and member states. Not by UN-compatible standards (such as UN/CEFACT) are the Reference points named which are considered useful to indicate the giant audience of international alignment and translation of data.

2.Information Systems

Contemporary Scenario(0-1 year)

Among some of the systems that are already in place are Transport Management Systems (TMS) used for transport execution and planning,Fleet Management Systems (FMS) involved in the state of vehicle condition, fuel use, location, and work-related operations of the vehicle,Enterprise Resource Planning (ERP) present in logistics firms as functionality is within business process integration, Port Community Systems (PCS) used for coordination by different stakeholders at the port level, Truck Appointment Systems (TAS) is an existing but poorly developed and jammed. Not fully integrated across fleets,Warehouse Management Systems (WMS) are peripheral systems that interact with ERP or consignment data flows,eCMR Platforms used for generating and managing digital consignment notes.

Future Scenario (5–10 years)

The interviewee expects future logistics systems to be smarter, more connected, and harmonized.Enhanced TMS and FMS platforms with advanced features like intelligent tracking, diagnostics, and route optimization.Gatekeeping with eFTI datasets which will define how data on each transport leg or event is structured and exchanged.Consignment note platforms becoming standard interfaces for structured data submission.Builder methodologies and use cases for the consistent understanding and application of system logic amongst IT developers. Policy makers and drivers.

3.Information Security

Contemporary Scenario(0-1 year)

The prevalent practices in information security are currently shaped by regulations such as the General Data Protection Regulation (GDPR), selective adoption of ISO cybersecurity standards, and policies with a national outlook on cybersecurity. These policies are applied variously among stakeholders and systems like TMS (Transport Management Systems), ERP (Enterprise Resource Planning), and Port Community Systems (PCS). Access controls and encryptions are implemented, though fairly inconsistently, mainly in case of small and medium enterprises (SMEs).

Future Scenario (5–10 years)

Future security frameworks will be expected to implement Zero Trust Architecture (ZTA) so that the credibility and trust of every data access will be established prior to giving a basis of permission. Role-based access control, real-time encryption, and querying of logged data shall be enforced at the system end. Cybersecurity compliance will be streamlined with the guidance of the EU's NIS directive, the revised ISO 27001 standard, and monitoring tools powered by AI that ensure real-time detection of threats and anomalies.

RQ2

1. Information Standards

Contemporary Scenario(0-1 year)

Intelligent Access implementation is hampered by inconsistent patterns of application and partial functionality of these current standards. IA is based on accurate, structured, and interoperable data for

automatically taking access decisions, route validation, and digital checks for compliance. The disparity of eCMR and limited enforcement of digital documentation standards has culminated in fractured data flows, rendering IA systems difficult to trust and work with. The reluctance from stakeholders to embrace IA processes arises from the lack of guarantees provided by underlying standards for uniform recognition across borders and authorities.

Future Scenario (5–10 years)
The future of these standards would have a transformational intent to facilitate IA. eFTI datasets and their harmonization will allow IA systems access in real time to transport information that has been verified so that authorities can securely, logically, and on a permissioned basis query against it. The automated compliance checks, IA, geofenced access, and terminal entry based on real-time access to vehicle and consignment data will be possible. With standardization in place, enabling cross-border IA functionality will provide reduced administrative overhead and create confidence among logistic stakeholders.

2.Information Systems
Contemporary Scenario(0-1 year)
Intelligent Access (IA) is not well integrated or standardized enough to ensure broadly applicable functionality. The interviewee stressed that the disconnection of these instruments made consolidated digital checks and automated terminal access impossible. If different authorities and systems demand different formats from IA functionality, redundant checks and fragmented data flows will develop. Such fragmentation works against the core principle of real-time validation of data logically throughout the supply chain, which includes fragmented checks and disjointed data flow.

Future Scenario (5–10 years)
In future development, this would lead to proper logical structuring of data flows with lower numbers of redundant checks. Due to seamless interaction of systems, object managers will no longer be checked six times across disparate systems. Data will be accessed in a consolidated manner; as a result, more effective real-time IA functionalities such as automated terminal entry, trip validation, and roadside inspection will be provided. Ulrika added that 5G, scanner, and onboard reader systems would augment mobile access validation for added proof of IA in streamlined and secure transport management.

3.Information Security
Contemporary Scenario(0-1 year)
Lackluster data sharing arrangements limit interoperability and trust between stakeholders in this current fragmented and non-mandatory approach to information security practice. The existence of data protection and security mechanisms uniformly and to a defacto standard will allow stakeholders to reveal sensitive vehicle, driver, or consignment data, thus providing IA with the necessary framework for acceptance in the road environment or terminal.

Future Scenario (5–10 years)
Latest Security advancements will enable Intelligent Access to be immensely scalable, reliable, and accurate, allowing Authority personnel to perform roadside checks to ascertain the validity of digital permits and confirm load and vehicle compliance by making secure real-time data queries without infringing on privacy laws. Systems will ensure, in the words of Ulrika, that access is granted only to relevant data specific to the use-case (for example, QR code-based access checks) that confine further extension and tracking of unauthorized nature. This will engender trust, enable automation, and foster

quick digital transformation logistics operations, with IA as the cornerstone of compliant and transparent freight movement across borders and nodes.

Expert 7

Title: Consultant and advisor specializing in digital logistics and artificial intelligence

Contemporary Scenario(0-1 year)
In the current situation, Intelligent Access (IA) is applied via AI-based systems that can assume complex logistical roles such as handling container logistics, identifying operation bottlenecks, and optimizing gate access utilizing license plate recognition. The applications allow for round-the-clock operations, reduce human errors, and improve overall throughput in road transport and freight terminal sectors. Technologies such as geofencing and real-time monitoring also make it easier to manage access dynamically and efficiently.

Future Scenario (5–10 years)
In the years to come, IA is likely to develop into an even more scalable and prescriptive framework. By being able to train AI models once and implement them in multiple logistics contexts, IA systems will become much more autonomous. Such systems will make dynamic decisions like adjusting access authorizations depending on the prevailing congestion, weather conditions, or priority of cargo using real-time data. Self-learning AI modules and real-time data connectivity will be the foundation of creating an intelligent, adaptive logistics ecosystem. Automated parking and charging slot bookings and predictive scheduling will facilitate more responsive and agile logistics operations.

RQ1

1. Information Standards
Contemporary Scenario(0-1 year)
The introduction of new standards for digital documentation, in particular for electronic consignment notes, is gaining acceptance in a number of countries worldwide. Such standardization aims to legitimize and digitalize certain transport documents which have for long been in use under paper-based regimes. Unfortunately, adoption does not take place in unison: several regions are still at a nascent stage of implementation.

Future Scenario (5–10 years)
The futuristic standards will be more dynamic, real time, and event-driven, thus directly supporting the scalability and sophistication of IA systems. The interviews point toward the demand for standards that will require a shift from a static document mode to a live trip-based data exchange, such as Real-time data formats for cargo updates and route changes, Protocols are harmonized at the EU level for interoperability across borders and Standard APIs for plug-and-play integration of various systems such as TMS, PCS, and terminal control platform.

2.Information Systems
Contemporary Scenario(0-1 year)
At the moment, logistics operations operate on systems such as the Port Community Systems (PCS) and Transport Management Systems (TMS) to coordinate freight movement and access. However, these systems are not uniformly accepted in different regions or by various stakeholders; thus, digital maturity is, therefore, at numerous levels. Geofencing enables the delimitation for controlling entry

through automated means, based on location. RFID technologies are used for data storage and transmission based on radio-frequency electromagnetic fields, thereby replacing the traditional barcodes with a faster and contactless way to verify the cargo.

Future Scenario (5–10 years)
AI will take Intelligent Access into the next era as more and more logistics platforms adopt it. Once trained, they will reliably be able to perform the same work in multiple environments. More consistent automation will be available through these systems. Automatic gates (with license plate recognition technologies) will allow real-time, contactless verification when accessing, reducing the need for intervention. New integrations with GPS technologies and connectivity solutions will allow for real-time data flow from vehicle to terminal.

3.Information Security
Contemporary Scenario(0-1 year)
Currently, there is little awareness of information security among many actors in road freight and terminal logistics. There are certain systems like access control on gates and elementary data protection mechanisms, but a holistic cybersecurity framework is lacking. Regulatory oversight especially from governing bodies is slow moving, resulting in the inconsistent way by which data security is managed in different logistics networks.

Future Scenario (5–10 years)
For scalable and dependable Intelligent Access, information security will become stronger over the years. Such utilities should comprise automated gate verification, automatic booking of charging and parking places, and real-time data exchange among logistics actors. Middleware systems will likely incorporate their evolutionary capability towards being embedded protections for connected infrastructures-from vehicles and roadside to terminal databases.

RQ2

1. Information Standards
Contemporary Scenario(0-1 year)
Impact of current standards in intelligent access are Assist Basic Levels of Digital Interoperability which means Standards like eCMR allow systems to share transport data in a more reliable fashion so that automated making of access decisions can happen at terminals, checkpoints, and border crossings. Improve Operational Efficiency which means these standards facilitate gate entries, curtail turnaround time in terms of minutes instead of hours, and assist IA systems in carrying out checks on the digital documentation as well as cargo and trip legitimacy.
However, the unripe and uneven application of these standards does not allow giving its full due for promoting intelligent access across regions and actors.

Future Scenario (5–10 years)
Standards in the future will influence Intelligent Access in the ways Via Prediction and Automation of Access Control. Under live continuous feeds and common structures of data, IA systems shall dynamically grant permissions depending on live data such as cargo status, environmental conditions, and traffic conditions. Enabling Interoperability among Systems and Supporting Smaller Operators with Some low-cost, easy-to-implement standards will encourage SMEs to participate in Intelligent Access schemes, thus fostering wider digital inclusion along the supply chain.

2.Information Systems

Contemporary Scenario(0-1 year)

The systems support Intelligent Access by enabling automatic gate processes, bottleneck detection, and overall improvement of vehicle and cargo flow processes at terminals. However, their low low integration across systems and inconsistent adoption prevented them from being widely effective in providing Intelligent Access capabilities.

Future Scenario (5–10 years)

Future platforms will have such functionality as digital booking of charging spaces and lots, with such features as automatically calculating energy needs (e.g., kWh) directly related to access management. This advancement will make access decisions much more real-time, responsive, anticipatory, and autonomous, yet will improve throughput, real-time adaptability, and increased intelligent coordination across road freight and port-terminal logistics systems.

3.Information Security

Contemporary Scenario(0-1 year)

The meager security infrastructure directly affects Intelligent Access by eroding trust among stakeholders and making it more prone to possible misuse or unauthorized access. It undermines the real-time exchange of sensitive information like the location of the vehicle, cargo information, and identity verification. Hence, the potential risk is reduced effectiveness and reliability of IA applications.

Future Scenario (5–10 years)

More powerful information security will enable IA systems to operate more like mono points for access verification and complete prevention to unauthorized persons from entering data-integrity modules. Not only will this progress the safety and efficiency of traffic flows, so it would also ease the implementation of digital and AI-powered access regimes in road and port terminal environments.

Expert 8

Title: Senior Representatives from ACEA (European Automobile Manufacturers Association)

Contemporary Scenario(0-1 year)

Today, Intelligent Access (IA) is in an early but functioning phase, evidenced in limited uses like geofencing, where the behavior of vehicles—such as speed—is automatically modified according to geography. This illustrates that digital access rules may be applied in particular, contained settings. Though the strategic value of IA is understood, particularly in supporting decarbonization objectives, its implementation is limited by decentralized policy environments and the absence of unified operational platforms across regions. Stakeholder participation with IA is still largely theoretical, and the systems underpinning it are not yet optimally integrated into day-to-day logistics operations.

Future Scenario (5–10 years)

In the coming years, IA will be one of the primary access management mechanisms for infrastructure access based on dynamic parameters such as vehicle emissions, safety scores, or efficiency. The aspiration is granting selective rights of access to cleaner, safer, or more efficient freight vehicles in order to reach climate objectives and streamline traffic.Real-time data systems and policy harmonization will be key to such evolution, allowing IA to facilitate seamless multimodal transport, traffic management, and enhanced cross-border operations. This potential, though, hinges

significantly on addressing existing shortcomings in standardization, interoperability, and policy coordination.

RQ1

1. Information Standards

Contemporary Scenario(0-1 year)

It is basic that eCMR and eFTI are information standards pertaining to the field of logistics. Digitization of freight documentation and compliance with European cross-border data exchange regulations are meant to ensure all the mentioned standards. Using only these standards in some areas has led to their practical application in Intelligent Access systems, as revealed by the interview. The experts suggest that even more direct insights into implementation could be achieved from associations of the industry like IRU or ERTICO, meaning that ther still is widespread adoption and operational integration of these.

Future Scenario (5–10 years)

While these specific future standards were unconfirmed at the time of the interview, they suggested that the next-generation standards for digital freight will be significant to the evolution of Intelligent Access. Examples include the further development and operationalization of eFTI and eCMR and the other system data exchange models being suggested under EU regulatory frameworks like the Intelligent Transport Systems (ITS) Directive. The above-mentioned standards will enable data sharing across logistics actors such as road operators, terminals, public authorities, and fleet managers that are machine-readable and in real-time. The future swings toward trip-based data structures, where transport event information, cargo data, and vehicle credentials will be digitally standardized and exchanged in real-time along the whole of the transport chain.

2.Information Systems

Contemporary Scenario(0-1 year)

The logistics are still functioning on a set of independent and often very limited systems that just keep their various parts operating- road freight and port-terminal operations. These include Transport Management Systems (TMS), Fleet Management Systems (FMS), Port Community Systems (PCS), Terminal Operating Systems (TOS), and Truck Appointment Systems (TAS). While operational all, this framework can provide operations support; it will never be able to lay the required ground for Intelligent Access because of a lack of real-time data exchange and interoperability among these systems. Most of the time, IA decisions (like granting access based on vehicle type or cargo) work manually on checking the data from these systems.

Future Scenario (5–10 years)

In the coming years, logistics and transport ecosystems are expected to adopt more intelligent, integrated, and data-driven systems. Future developments will mostly showcase AI-powered platforms, systems integrated with the IoT, Cloud-based systems, Modular and Interoperable Systems, as it would be related to the interview. These systems are geared towards having direct interfacing with IA frameworks, thus receiving real-time validated data streams for reliable rule-based access control.

3.Information Security

Contemporary Scenario(0-1 year)

From the interviewee's perspective, information security today is treated on a manufacturer-by-manufacturer basis without any common or cross-sector standards. The security infrastructure basically comprises elementary encryption schemes, some manual access control, and cloud-based authentication systems for securing vehicle telematics and backend logistics platforms. ACEA-as an advocacy system-is not directly concerned with the implementation of security technologies. In turn, different manufacturers deploy different proprietary cybersecurity protocols that have varying levels of rigor and design, and therefore the current state of information security is very much a fragmented process with inconsistent levels of protection among stakeholders in the road and port logistics chain.

Future Scenario (5–10 years)

Systems that access intelligent futures shall be formed on advanced, standardized, and interoperable cybersecurity frameworks. Though those interviewed had not mentioned any technological specificity, there were hints towards an impending need for such measures as Zero-trust architecture, requiring continuous authentication of users and systems; secure telematics; and real-time intrusion detection systems. Such security models will be fundamental to the management of confidential logistics data from unauthorized access and the protection of communications amongst vehicles, terminals, and public authorities. In addition, the connected systems and automated platforms increasingly applied within IA will mean moving beyond isolated security implementations into durable, sector-wide data protection regimes. Progressive emerging information security frames will reshape Intelligent Access with trusted, real-time information exchange within the entire logistics ecosystem.

RQ2

1. Information Standards

Contemporary Scenario(0-1 year)

As such, without being additive to and with the incomplete and irregular implementation, the current information standards provide a limited application for Intelligent Access in road freight and port-terminal logistics. Hence, without real-time structured interoperable data, IA cannot assess a vehicle's compliance, cargo status, or emission category automatically. This leads to an access validation process that is mostly manual and reduces the efficiency and scalability of IA frameworks. It may be seen that this limited operational use of eCMR and eFTI restricts the potential of dynamic, rule-based access control enforcement by IA in addition to its other wider burdens like decarbonization, digital compliance, and logistical coordination.

Future Scenario (5–10 years)

The next generation of information standards will vastly improve the capability and reliability, not to say efficiency, of Intelligent Access systems. With these structured and automated data flows, IA will dynamically check vehicle and cargo eligibility using standardized inputs such as emissions class, cargo type, and routing data. Ultimately, this will lead to a decreased need for manual documentation and physical inspection, rendering access control more effective, faster, and scalable. Moreover, harmonized standards will provide cross-border interoperability, which is of utmost importance for international freight corridors and port commodities. Thus, seamless data exchange among the standards will facilitate IA with environmental compliance, decongestion, and optimal infrastructure utilization across road and port-terminal environments.

2.Information Systems

Contemporary Scenario(0-1 year)

The contemporary generation of information systems does not maximize Intelligent Access at all since they are scattered and poorly integrated. Real-time data about vehicle identity, cargo type, permits, or emissions class, do not flow - as they typically do in silos - among authorities, terminals, and transport operators. This is a limitation that prevents IA frameworks from making dynamic, automated access decisions based on predefined criteria. Therefore, today, the implementation of IA uses a piecemeal approach, with a kinetic-like static manual process, thus leading to a lot of inefficiencies in gate operations, time lags caused by cross-docking, and difficulties in enforcing policies such as low-emission zones or high-priority cargo lanes.

Future Scenario (5–10 years)

Future applications will be incredibly accurate, scalable, and adaptable for Intelligent Access in road freight and port-terminal environments alike. This is automatic evaluation based on integrated, real-time information providing that IA will instantly allow or deny access according to compliance, risk assessments of cargo, or operational priorities. Fast throughput gates at terminals and ports; Smarter allocation of infrastructure capacity according to emissions, cargo type, or urgency; Better enforcement of environmental and safety regulations through automated access restrictions; and, finally, Improved coordination between transport modes will enable multimodal IA applications. The use of advanced information systems will ultimately make Intelligent Access the core enabler of sustainable, efficient, and transparent logistics operations.

3.Information Security

Contemporary Scenario(0-1 year)

The lack of standardized and interoperable information security hinders, in contemporary logistics, scaling and dependably applying Intelligent Access systems. On account of the variations in data protection frameworks between operators or systems, stakeholders resist sharing sensitive information, i.e. vehicle location, cargo details, and access credentials. Such resistance undermines real-time decision-making, hampers automation of access control, and delays IA acceptance across critical nodes such as ports and terminal gates. Added to that, any breach of data confidentiality or unauthorized access into logistics systems dent any trust into this more extensive ecosystem. Hence, ecosystem-wise, the IA has been only partly applied and is still manually operated-rather than being a fully dynamic, secure, and integrated modus operandi for transport access regulation.

Future Scenario (5–10 years)

Strong cyber security will give that possibility to the automatic validation of the vehicle credentials in IA systems, dynamic access rules enforcement, and sensitive zones such as ports, terminals, or urban low-emission areas management. Secure systems will also help satisfy regulatory requirements regarding data privacy and liability, thus increasing confidence and involvement of the different stakeholders. Thus, Intelligent Access will be a scalable and reliable framework for managing access to transport, which will provide support for goals like decarbonization, congestion control, and multimodal coordination across road freight and port-terminal logistics.

Good examples of eFTI and eCMR implementations

Several strong pilot initiatives and legislation across Europe demonstrate the practical efficiency of eFTI and eCMR in digitalizing logistics and Intelligent Access (IA) development:

Italy e-CMR Pilot Initiatives: Gruber Logistics, among others, tested eCMR for transport of medicines. The pilot demonstrated interoperability and efficiency benefits, particularly in high-sensitivity logistics chains.

Open Logistics Foundation's Lighthouse Project (Germany): Over 150 shipments were tested successfully by leveraging an open-source eCMR solution in live operational environments, validating the scalability and reliability of the standard.

Eurasian Economic Union e-CMR Pilot: Eurasian Economic Commission's multinational pilot on eCMR tested eCMR among EAEU member countries to direct attention towards efficient cross-border logistics.

Bolk Transport (Netherlands): In 2019, this Dutch company implemented eCMR, which delivers instant document accessibility and optimized loading/unloading by TransFollow. Bolk was also involved in the Intelligent Access pilot in the Netherlands and employed data merged with eCMR for data-driven access management without compromising data privacy.

Smart Multimodal Operations Platform (SMIP) of the Netherlands: A key pilot site for EU4Digital to deploy eFTI, SMIP enables multimodal freight data exchange under the eFTI Regulation.

Germany – eFTI4EU Pilot: Germany, under the eFTI4EU initiative, developed an open-source eFTI reference implementation integrating eCMR data and an Authority Access Point for real-time communication of authorities.

Finland – eFTI Gate Proof of Concept: Finland's PoC, initiated by Traficom, for the development of a national eFTI gate, was tested in pilot with logistics stakeholders to ensure technical readiness.

Western Balkans – Roadmap for eFTI Implementation: Guided by the Transport Community, it aims to outline phased eFTI implementation in the region, aspiring to be aligned with EU digitalizing of logistics initiatives.

Spain – Legislative Push for Mandatory eCMR: Spain is completing its Sustainable Mobility Law, imposing mandatory use of eCMR for road freight towards the close of 2024, as an evidence of legal harmonization of EU digital policy.

A reference table with detail and link to each of the projects is available in Appendix B – Reference Table of eFTI and eCMR Case Examples.

5. Analysis

The analysis highlights how the problems identified in the problem statement such as lack of coordinated system integration, fragmented data exchange, and inadequate information security are addressed through a systematic evaluation of digital enablers. These problems, which hinder real-time coordination, delay terminal operations, and risk regulatory non-compliance, were investigated through an approach that combined a comprehensive literature review with eight semi-structured expert interviews. One of the main analytical instruments for comparing in a systematic way how these three enablers are perceived and realized across various logistics environments was the methodology table, which categorized each expert's contribution according to information standards, systems, and security dimensions. The structured character enabled cross-validation of shared problems such as low interoperability and insufficient digital readiness, particularly among small and medium operators. The empirical findings provided us with real-world feedback from industry professionals who confirmed that these problems are not autonomous but interconnected, and in most instances, concurrent developments in digital documentation, system integration, and secure data exchange are required. In this research, we will therefore examine which types of information standards, systems, and security measures are most suitable to tackle specific logistic problems. By mapping every enabler to the problem domain involved, the analysis aims at describing how digital solutions may be applied in a targeted manner to enable Intelligent Access (IA) and support more efficient, synchronized, and trustworthy logistics operations.

What information standards, information systems, and information security measures can be applied both contemporarily and in future scenarios for intelligent access in road freight transport and port-terminal logistics? How do these contemporary and future planned standards, systems, and security measures impact intelligent access in these logistics domains?

5.1 Contemporary Information Standards

	Road hauliers 	Smart roads: Highways 	Smart parking 	Smart roads: Cities 	Terminals / Ports 
Information standards	B2B,opentripmodel(OTM),Eurostat	B2B,G2B, B2G, AutoTRIX,NAP, Eurostat	NAP	B2b,G2B, B2G,AutoTRIX,NAP, Eurostat	B2B, RFID,EDI,NAP
Information systems	FMS, ERP	TMS, FMS		TMS, FMS	PCS, TAS,TOS
Information security	RFID,EDI				ZTA,AMS,RFID,EDI

Fig. 1 Contemporary Scenario(0-1 year)

1. Electronic Data Interchange (EDI)
A well-established EDI is found in the road haulier, port, and terminal domains due to its automating role in exchanging logistics documents between the main actors, such as customs, transport operators, or terminal managers. With road freight, EDI enables consignments to be digitally processed, customs to be cleared, compliance to be checked, and reduction of manual processing in road freight. Port-terminal operations support gate-in/gate-out procedures, container tracking, and integration of Terminal Operating System (TOS) for Intelligent Access (IA) with structured machine-readable data that access control systems can automatically use to check for compliance, thereby allowing only vehicles and shipments meeting the requirements to be allowed to enter. This automation eliminates delay and enables predictability along with security.

Interviewees have considered EDI as the digital standard beneath interoperability and consistent communication among logistics systems; they stressed its relevance today, particularly in relation to IA validation and system-to-system integration. This opinion is reiterated by most of the literature, most notably in the study done by Heilig and Voß (2016), which validates the importance of EDI for maintaining operational consistency and enabling automated access decisions within logistics networks.

2. Radio Frequency Identification (RFID)
The current setup denotes RFID in under road haulage and port/terminal domains due to its use in real-time tracking of vehicles, containers, and cargo (Imburgia, 2006; Dasaklis et al., 2024). In ports, RFID facilitates automated gate entries, container movements, and interfacing with Terminal Operating Systems. Road transport allows it for vehicle and cargo verifications by customs and checkpoints, thus avoiding delays.

RFID contributes to IA by enhancing the visibility of operations, restraining idle times, and allowing secure and real-time decision on access. Experts consider its contribution to dynamic access control in a terminal setting. This corresponds to literature confirming the value of RFID in improving logistics and automating access.

3. B2B, B2G, G2B Platforms
These are B2B, G2B, and B2G interfaces existing today across road haulier, port/terminal, smart roads: highway and cities, as well as in smart parking domains due to their paramount role in real-time data interchange between businesses and government authorities. They support IA by means of permits, compliance checks, and schedules.

In road freight, they furnish licenses for transport authorization. For ports, they dispose of customs and cargo clearance. In cities and parking domains, these interfaces allow for emission zone access and time-slot controls. Experts felt that these systems are used more and more by municipalities for the analysis of eligibility for IA. This goes especially with the European Commission (2020), which sees merit in using these platforms for competent cross-border logistics and regulatory enforcement.

4. Open Trip Model (OTM)
In contemporary Scenario, OTM can be categorized under the domain of road haulage as an information standard to organize trip, vehicle, and routing data in real-time and support the operational requirements of Intelligent Access (IA) (OpenTripModel.org, n.d.). In contrast with more traditional standards such as EDI, OTM adds to IA by allowing dynamic, event-based logistics wherein access decisions can be made on the basis of vehicle attributes, emissions, load type, and time slot authorizations.

OTM allows the real-time communication of data with TAS and V2I systems, serving as a base layer for automated rule-based IA. Experts view OTM as very flexible and able to marry policy with routing logic, which makes it a lot more adaptable than rigid legacy standards. Although its use in the logistics setting is already documented, literature has yet to explore OTM in its IA capacity, thus marking the expert insights as an exceedingly useful forward-looking insight (Aventeon, 2023; OTM Developer Portal, 2023).

5. AutoTRIX

AutoTRIX falls under the category of intelligent roads, including highways and cities, since it was specifically designed to control abnormal and oversized transport movements through an automated permitting and routing system. In the example in Sweden, AutoTRIX is an instrument applied under Intelligent Access (IA) to make decisions about access in real time, based on the characteristics of a vehicle and infrastructure constraints. It uses live traffic data and smart infrastructure inputs to establish a route's eligibility and to issue permits automatically. This automated permit process helps maintain infrastructure integrity and transport efficiency, especially for oversized and heavy vehicles. According to experts, it is their strongest suit to one of the ways in which the automation of access decisions for high-capacity vehicles can take place, allowing authorities to ensure safety and infrastructure protection while promoting efficient transport operations.

6.National access points(NAP)

NAPs are located in smart roads in the highways and cities category, smart parking, or Port-terminal category, as these are primary control points in logistics that require data interchange by a standard on a real-time basis in order to have coordinated and secure access control. On highways, NAPs under delegated regulation (EU) 962/2015 provide real-time traffic information (RTTI) so that the Transport Management Systems (TMS) and Fleet Management Systems (FMS) may better optimize routes based on information about incidents, speed limits, and congestion (Aifantopoulou et al., 2020; European Commission, 2024). In city roads, NAPs provide access to low emission zones, delivery windows, and multimodal transport options under Multimodal Travel Information Services (MMTIS) regulation (EU) 2017/1926 and enable logistics actors to digitally comply with such complex urban access regulations (EPRS, 2021). In smart parking, NAPs publish real-time information about parking availability and metadata on safety features under the Safe and Secure Truck Parking (SSTP) initiative of Regulation 885/2013, which helps to prevent illegal parking and promote compliance by truck drivers (Hendriks et al., 2018). Traditionally, terminals and ports rely on PCS and TOS systems; however, NAPs are increasingly important for integrating last-mile road data such as access slots and congestion indicators as part of the digital interface between road and port operations (TRA, 2022; Mylonas et al., 2023).Literature strongly agrees with this placement, consistently identifying NAPs as key to improving data interoperability, logistics efficiency, and regulatory compliance in the contemporary logistics environment.

7. Eurostat

Eurostat falls under the information standards domain for Road Hauliers and Smart Roads (Highways and Cities) in the current scenario because it provides the harmonized statistical frameworks necessary for creating and comparing transport-related activities across the EU. This distribution is justified by the role of Eurostat in facilitating harmonized business-to-business (B2B), government-to-business (G2B), and business-to-government (B2G) information exchanges supporting road haulage operational and regulatory processes as well as intelligent road infrastructure (Eurostat, 2022). Such information standards are required to deliver a common language and format to report freight flows, usage of road networks, and mobility performance of the member states.

Within Road Hauliers' context, Eurostat supports information standards with NACE use in classification and through the use of harmonized measures for freight quantity, vehicle categories, and size of enterprise. This improves structured B2B data flows as well as the integration of external trip and event knowledge models such as the OpenTripModel (OTM), which depends on statistically valid and semantically coherent data inputs in route optimization and cargo tracing (Eurostat, 2000). For Smart Highways – Cities and Highways, Eurostat's reachability indicators such as population reachability within specified drive time ranges offer a shared metric for evaluating road network performance across cities and highways (Dijkstra, Poelman, & Ackermans, 2019). These indicators support both B2G and G2B interactions by offering cities and governments at the national level a standardized framework to evaluate road use and connectivity.
Existing literature supports this analysis Dijkstra et al. (2019) argue that traditional speed and capacity measures are incomplete without harmonized accessibility information, and that Eurostat's cumulative opportunity approaches give better reflective and policy-relevant pointers to transport performance. The literature is thus in agreement that Eurostat's pioneering role in setting information standards is the foundation upon which information-based road transport policy is enabled within both logistics and infrastructure industries.

5.2 Contemporary Information Systems

1. Port Community System (PCS)
Port Community Systems (PCS) stand today under the port and terminal sphere of activity since their recognized use is in integrating various port stakeholders in a single digital platform such as customs, terminal operators, and shipping lines (Heilig & Voß, 2016). These systems are expected to handle the main port operations, such as gate automation, berth scheduling, and customs declaration, all of which are indispensable when it comes to coordinating terminal access and cargo flow.

PCS contributes to IA by allowing timely and secured data transmission by which vehicles and cargo may be checked for compliance before entry, hence lessening gate delays and ensuring access control. It may also be utilized in the coordination with road hauliers to plan for arrivals definitively and in synchronizing arrivals, which is a consideration in ensuring operational efficiency at a busy terminal.

Experts have stressed the importance of PCS in improving electronic visibility and pre-verification access, thereby allowing faster, rule-based decisions for vehicle entries into terminal zones. The views abided by the literature, which indeed sees PCS as a prime enabler of port digitalization and a provider system for setting up IA within port ecosystems (Heilig & Voß, 2016).

2. Transport Management System (TMS)
In the present setup, the Transport Management System is considered under road haulier and smart roads: highways and cities domains because they are mostly used to handle the freight logistics side of operations, from routing, dispatching to shipment tracking, and cost optimization (Drljača & Sesar, 2023; More et al., 2022). This real-time modulation of decisions makes their coordination with logistics operations an absolute necessity for supporting Intelligent Access where enforced routing must be delivered on time.

In the road haulier domain, TMS supports carriers in planning their routes that comply with regulatory requirements, manage delivery schedules, and optimize transport costs. In smart roads and cities, the TMS navigation through low-emission zones is adjusted to time-based restrictions and integrates dynamically-restricted areas with real-time traffic systems via APIs and IoT platforms to disperse

congestion and improve delivery efficiency. This further assists IA by allowing vehicles to adapt their movement according to the dynamic access conditions.

According to the interviewed experts, TMS is in increasing interaction with smart infrastructure, though certain issues persisted with fragmented standards in the data and limited interoperability into urban systems. These insights are backed by the existing literature, wherein TMS is seen as the backbone of transport logistics and a major contributor to delivery performance, cost efficiency, and compliance (Drljača & Sesar, 2023; More et al., 2022). Thus, positioning TMS in these realms for the modern-day scenario corresponds to expert practice and academic findings alike.

3. Fleet Management System (FMS)
Due to their extensive application in real-time vehicle monitoring, compliance tracking, and predictive maintenance, fleet management systems are currently classified under the road hauler and smart roads: highways and cities domains (Shivkumar & Supriya, 2024). In road freight, FMS enhances IA by providing the ability to track the location of vehicles, conditions, fuel consumption, and driver behavior to effect safe and efficient operations. In smart road environments, FMS works with geofencing, traffic signals, and emission zones to provide compliant routing and adaptive access control. FMS was found by experts to be a very significant enabler of IA by providing real-time vehicle-infrastructure communication for route planning and access validation. The literature supports this perspective by highlighting how FMS minimizes on-site downtime and optimizes delivery through the integration of IoT and platforms such as ThingSpeak cloud (Challa, 2016; Shivkumar & Supriya, 2024).

4. Truck Appointment System (TAS)
In contemporary scenarios, truck-appointment-based systems have been placed under port/terminal environments since they broadly apply to truck-arrival-congestion management, gate-congestion reduction, and yard operation enhancement (Lange et al., 2022). Time slots are assigned to trucks by the TAS, which should allow better planning of resources and smoother cargo handling at the terminal.

A TAS which functions under IA principles will help reduce emissions alongside idle time by restricting truck access to those that have scheduled appointments with cargo information (Im et al., 2021). Terminal operators and hauliers require the TAS system for real-time coordination despite its current inflexible and disjointed interface with haulier restrictions (Phan & Kim, 2016; Ericsson & Svensson, 2022). The benefits of TAS systems receive recognition from practitioners but they also identify the system's inflexibility together with its demand for adaptability.

5. Terminal Operating System (TOS)
As per Min et al., 2017, in today's times, Terminal Operating Systems (TOSs) fall under the port/terminal type since they are largely used for container flow management, berth planning, and gate operations at ports and terminals. In the context of Intelligent Access (IA), TOS enables trucks to access in a controlled manner where the trucks are permitted entry based on a time slot and cargo documents, particularly if TOSs are accompanied by TAS and PCS (Heilig & Voß, 2016).

The experts are of the view that TOSs provide the automation of the process of the gate access control and also the authorization of the incoming vehicles that makes the system more efficient and less congested. It is stated that TOS is essential for the movement of the freight through the smart terminal, the advanced communication based on the EDI and the planning tools integrated with AI to achieve the port efficiency in real-time (Choi et al., 2003; Zimmerman et al., 2021).

6. Enterprise Resource Planning (ERP)
ERP systems are categorized under the road haulier domain of the current set-up, owing to their capacity to integrate all logistics functions such as transport planning, inventory, customs, and finance into one interface (Aremu et al., 2018). Hence, this endows complete supply chain visibility and supports Intelligent Access (IA) by aggregating vehicle, cargo, and scheduling data for coordination with systems like TMS or TAS.

Experts averred that the ERP systems guarantee that compliant vehicles are dispatched, accompanied by legitimate documentation, thereby strengthening the logistics coordination internally and externally. In the literature, it was further illustrated by the authors that the ERP system handles logistics operations, making data available in real-time on a cloud-based platform for the effective execution of transport activities (Aremu et al., 2018; Ebirim et al., 2024).

5.3 Contemporary Information Security

1. RFID and EDI
A security system can be at the highest level of land cargo information standards in the present-day situation. RFID may contain aspects of security for physical assaults against gate access, vehicle and cargo verification, and tampering detection in road freight, while in ports, it supports container tracking and access control. EDI ensures the secure exchange of transport documents through encryption, timestamping, and auditability (Imburgia, 2006; Shie et al., 2011).

The participants expressed the opinion that RFID is indispensable when bridging physical and digital systems in secure access with EDI ensuring secure communication amongst hauliers, ports, and authorities. These opinions support the literature that validates the ability of the two standards to aid secure and reliable Intelligent Access.

2. AWS Managed Services (AMS)
In the modern context, AWS Managed Services are placed under the port/terminal domain due to their increasing demand as a secure cloud infrastructure for hosting IA and port logistics systems. Its placement reflects the growing preference among modern terminals for cloud-based deployment of mission-critical systems that can support very high availability, scalability, and cybersecurity safeguards at a rigorous level (Amazon Web Services, Inc., 2025).

It supports IA through AMS by granting integrated services such as IAM, data encryption, and security audit to provide secured access control, cargo visibility, and scheduling of various stakeholders. The cloud-based solutions allow AMS to help in complying with GDPR and operational continuity without setting up further local infrastructure.

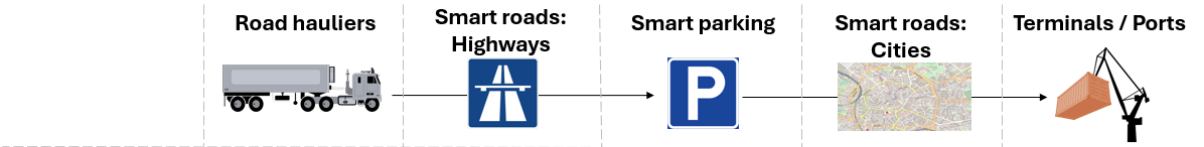
Experts indicated that AMS undergirds IA-related systems with adequate data protection and system resilience demanded by modern terminals; this is consistent with findings from recent technical reports that affirm the dominant use of AWS cloud services to operate secure and real-time logistics. Hence, expert views and the literature converge to confirm the standing of AMS in supporting modern port IA environments.

3. Zero Trust Architecture (ZTA)
In the current state of affairs, ZTA is considered a port/terminal security framework as it is an emerging discipline increasingly recommended to protect common digital systems with applications

of joint concern by multiple actors, e.g., customs, terminal operators, and hauliers (Kulkarni & Cheikhrouhou, 2024).

ZTA facilitates IA, thereby brooking strong identity verification, and enforcing least-privilege access across every interaction, thus securing systems such as PCS, TOS, and gate interfaces. Experts pointed to ZTA supporting role-working-based access accountably from other perspectives in relatively complex port scenarios. This can be viewed alongside literature advocating increased resilience for multi-stakeholder logistics with ZTA whilst only being scarcely applied today.

5.4 Future Information Standards



	Road hauliers	Smart roads: Highways	Smart parking	Smart roads: Cities	Terminals / Ports
Information standards	e-FTI, e-CMR	e-FTI,Datex II		e-FTI,Datex II	e-FTI, e-CMR
Information systems	Geofencing, ITS,V2V, V2I, I2V	Geofencing, ITS, V2I, I2V,V2V		Geofencing,V2I,I2V ITS,V2V	
Information security	AMS,ITS	GDPR,NIS2		GDPR,NIS2,	AMS,Json Web signatures,ITS

Fig.2 Future Scenario(5-10 year)

1. eFTI (Electronic Freight Transport Information)
In the future scenario, eFTI is set up under road haulier, smart roads: highways, and cities, and port/terminal domains due to its evolution toward a standardized, digital freight data exchange. It is mandated by EU Regulation 2020/1056, with full operational integration, especially for cross-border logistics, envisioned by 2027 (European Commission, 2020; 2025).

In road freight, eFTI provides for digital verification of permit and compliance. Under smart roads, it is used for real-time access control on permit basis using vehicle data. At the ports, it is linked with PCS and customs systems for expediting cargo clearance and minimizing errors (Chountalas et al., 2024).

Experts considered eFTI foundational for the future IA, supporting regulatory harmonization and trusted cross-border communication, while maintaining that there are still some issues to be addressed concerning the integration of legacy systems. The literature was unanimous in stating that eFTI would be a game changer and yet called for the development of standardized platforms that are interoperable (Heilig & Voß, 2016).

2. eCMR (Electronic Consignment Note)
The electronic consignment note (eCMR) lies with the road haulier domain and port/terminal domains in the future scenario, being able to replace old paper-based freight documentation systems with secure, digital alternatives. Adoption rates worldwide remain below 5% due to the lack of digital readiness among stakeholders throughout the chain of transport.

For road hauliers, the eCMR provides a real-time shipment information view, inter alia, facilitating compliance checks and cutting down on paper. And in ports, it complements integration with the Port Community Systems (PCS) and customs platforms to secure, traceable documentation of cargo and expedited clearance.

Experts pointed out issues surrounding eCMR's facilitation of logistics and support for digital IA systems, pointing out that factors affecting wider adoption will be regulatory alignment and shared infrastructure. The literature agrees; that is, while supporting the benefits of eCMR, it also recognizes the challenges of adoption faced today (Heilig & Voß, 2016).

3. Datex II
Placed under smart roads-highways and cities in the future scenario, Datex II serves as the standardized information model for real-time traffic and infrastructure data exchange, necessary for intermittent IA implementation. It facilitates the communication to vehicles and access control systems of road access rules, temporary restrictions, and incidents to allow automated routing and compliance verification.

Experts observed that Datex II is currently mostly used for traffic reporting; however, its role will grow as integrated digital access controls come to be employed by cities and highways. They established the possibility of Datex II to further real-time, rule-based IA decisions. These assertions are extracted from interviews, as a particular application of Datex II in IA contexts does not yet exist in the literature and is thus considered a new and emerging area of practice.

5.5 Future Information Systems

1. Geofencing
Geofencing belongs to the road haulier and smart road-highways-and-cities domains in the future scenario because of its potential to enable location-based Intelligent Access, despite its limited deployment at present. It is now mostly used in low-emission zones but is expected to see wider deployment in the next 5–10 years (Lindkvist et al., 2023).

Geofencing allows varying access issues to be controlled according to traffic, emissions, or time-based rules. For road hauliers, it acts to ensure compliance by dynamically adjusting the routes and access of vehicles as they approach zones where access is restricted.

Experts hence describe geofencing as a necessary building block of IA, forming rule-based access decisions in real-time, while noting the limitations still evident in its integration with TMS. This somewhat mirrors the literature, which also supports its potential but acknowledges its underutilization in freight logistics.

2. V2I, I2V, V2V (Vehicle-to-Infrastructure/Vehicle)
Given their potential to enable real-time and automated decision-making in IA, V2I, V2V, and I2V communications technologies are placed under the road haulier and smart roads: highways and cities domain in the future scenario. Even though their freight-specific applications are still rather limited (Williams, 2008), they are used in pilot programs.

Under smart roads, these allow access control on a dynamic basis, signal prioritization, and coordination of traffic. Within the road hauliers context, these allow for the real-time sharing of compliance and routing information for vehicles so that the infrastructure may grant or alter access.

Being recognized as an important enabler for the development of future IA, V2X is said to improve safety, emissions abatement, and efficiency despite the limited use so far. This is consistent with existing literature, which finds V2X most promising but also acknowledges that applying it to freight logistics has been slow (Dey et al., 2016).

3. ITS (Intelligent Transport Systems)
In the affected realm of road hauliers and smart roads-highways and cities-it is conceived that ITS will emerge as an enabler for data-driven, responsive freight access control. It is probably, and I stress probably, because V2X, adaptive signals, and dynamic tolls are being used in passenger mobility but have yet to take hold in freight operations (Hasan et al., 2013).

ITS-enabled smart roads allow the consideration of real-time traffic data and dynamic routing to grant access depending on time or congestion or road conditions. ITS, for road hauliers, enables route planning, emission regulation, and scheduling by interfacing vehicles to infrastructure.

ITS was discussed as a key enabler for future IA by the experts and at the same time pointed out the little use made of it in freight transport. This view corresponds to the literature which acknowledges ITS capabilities but highlights the slow uptake in logistics contexts.

5.6 Future Information Security

1. AMS (AWS Managed Services)
Under the proposed future scenario, under-road haulier and port/terminal are areas into which AMS is cast due to the need for secure compliant cloud infrastructure for logistics systems. These sectors deposit increased reliance on cloud platforms for handling sensitive information in routing, cargo tracking, and customs processing. Some manual systems of TMS, FMS, PCS, and TOS are supported by AMS with offerings such as Amazon GuardDuty, AWS Security Hub, and CloudWatch for real-time threat detection, access control, and compliance monitoring (Amazon Web Services, Inc., 2025).

Experts elaborated on the sustaining nature of AMS to enable the scaling of logistics operators securely while reducing cybersecurity-related risks, particularly with their IA systems becoming increasingly interconnected. Whereas AMS is not currently considered an industry standard, it is instead looked upon as a future-forward direction for implementing secured automated access, which is a viewpoint that extends beyond what is discussed in prior literature that deals with cloud adoption in logistics but pays limited attention to managed security services. This thus corroborates that expert insights add a new dimension to the understanding of AMS's future role in IA.

2. GDPR & NIS2 (Cybersecurity Directive)
GDPR and NIS2 are placed under the smart roads: highways and cities domain in the future scenario, as their roles are very important in governing data privacy and cybersecurity in Intelligent Access (IA) systems. As the smart infrastructure grows simultaneously with vehicle-infrastructure communication, IoT devices, geofencing, and real-time data exchange, both regulations will be crucial for making sure that access decisions are implemented securely, lawfully, and accountably.

GDPR, in a way, contributes to IA by protecting personal data such as vehicle location, identity, and behavioral patterns. It will have to handle much more complex issues in the future, for example, AI-based decision-making, blockchain recording, and cross-border data flows in logistics ecosystems (Zaeem & Barber, 2020; Li, Yu, & He, 2019). NIS2, keeping with this, strengthens the cybersecurity

risk management, supply chain security, and incident response to ensure the resilience of IA platforms on automated access control and predictive analytics (Mueck & Gaie, 2025; Singh, 2023).

Experts acknowledge that the GDPR is already well-known but lacks enforceability by way of real-time enforcement in smart mobility contexts, notably regarding consent and anonymization of live data. NIS2 was seen as the next critical step toward a harmonized cybersecurity practice framework across IA systems, especially as the threat landscape evolves and digital infrastructure becomes more decentralized.

This line of argument favors the expert assessment, which also considers the worldwide influence of the GDPR and recognizes the emerging role of the NIS2 on the security of essential transport services. Both are set to go far toward forming the basis of governance for future IA systems, thereby justifying their inclusion in future-oriented, data-driven transport environments (Heilig & Voß, 2016; European Commission, 2016; Mueck & Gaie, 2025).

3. JSON Web Signatures (JWS)

When it comes to logical port/terminal domains in the future, JWS has been placed in view of its importance as a component in securing decentralized communication in complex logistics environments such as ports and terminals. JWS permits events like cargo handovers or permission to be cryptographically signed and verified, doing away with central APIs for enhanced security, ease of system integration, and data tampering. Being part of IA, JWS authenticates data exchange arising from access credentials, compliance data, or risk assessments, mainly toward V2I systems. In the future, JWS will integrate with blockchain and digital twins for localized, tamper-proof verification of decentralized IA systems, guaranteeing real-time decision-making secured on demand. Experts feel that JWS is scalable and works well minimizing reliance on centralized security systems, thereby making it crucial to both reliable and efficient IA operations. This is supported by previous literature testifying to the importance of decentralized cryptographic signatures in minimizing vulnerabilities in multi-actor environments such as ports and terminals, further reinforcing JWS to be foundation to future IA security (Jones et al., 2015).

6. Discussion

The discussion chapter builds upon the problem description, methodology, and empirical findings to critically examine how information standards, systems, and security frameworks can cumulatively address the chronic issues in road freight and port-terminal logistics. As found in the problem description, issues of fragmented data exchange, uncoordinated system integration, and lack of information security continue to undermine operational efficiency, real-time coordination, and regulatory compliance. In attempting to research the issues, the study adopted a two-method approach through a targeted literature review and eight expert interviews, which supported both theoretical underpinning and empirical confirmation. The methodology table helped to structure expert opinion under the themes of standards, systems, and security, which allowed for a systematic comparison of how each digital enabler solves targeted problem areas. The empirical findings confirmed that while digitalization is underway, its uptake continues to be uneven particularly among small and medium operators due to lapses in standard uptake, system interoperability, and data protection. This discussion chapter will therefore explore how and to what extent these digital enablers can resolve the issues found, and also clarify what kinds of standards, systems, or security measures are most suitable for respective problem domains in the application context of Intelligent Access (IA).The discussion is framed across two temporal scenarios: contemporary (0–1 year) and future (5–10 years), allowing a clear comparative understanding of present practices and anticipated developments.

6.1 Contemporary Scenario(0-1 years)

Frameworks	Better use of existing infrastructure with traffic management based on time and place;	Less degradation of road infrastructure through improved management of weight, speed and routing of heavy vehicles;	Realizing climate objectives by reducing congestion and prioritizing climate-friendly vehicles, for example management of low emission zones, and this will give more transparent and greener logistics;	Increasing road safety through, for example, less overloading or improved insight into where safety incidents arise on the road network;	Creation of a level playing field between different haulers/carriers, improving compliance by haulers/carriers with regulations as set out by NRAs;	Improved control of the transport of abnormal loads and dangerous goods;	Controlled introduction of High Capacity Vehicles;	Faster and more unified and controlled processing of transport documents in cross-border transport through digitalization.
Information standards	OpenTripModel (OTM),Eurostat		Eurostat,NAP	NAP	OpenTripModel (OTM), G2B,B2G	OpenTripModel (OTM), G2B,B2G RFID,AutoTrix, Eurostat	G2B,B2G, AutoTrix	OpenTripModel (OTM), G2B,B2G RFID,EDI, Eurostat,NAP
Information systems	TMS,TAS	TMS,FMS	TMS,FMS,TAS	FMS,TMS	TAS,PCS	TMS,FMS		PCS,TMS,TOS, TAS,ERP
Information security					ZTA,AMS	ZTA,AMS		ZTA,AMS

Fig. 3 Contemporary Scenario for intelligent access(0-1 year)

1. Better Use of Existing Infrastructure with Traffic Management Based on Time and Place

To enhance the utilization of existing infrastructure, Intelligent Access (IA) requires time- and location-based traffic coordination. The OpenTripModel (OTM) standard is essential here, as it provides a flexible, semantic structure for sharing trip-level data such as vehicle position, weight, and route preferences as highlighted by the experts in the interview. This makes it possible to control and maximize when and where freight trucks enter specific roads or zones through governing bodies and systems. Truck Appointment Systems (TAS) and Transport Management Systems (TMS) provide operationalization of such access controls through facilitating the scheduling of deliveries by transport

planners based on available infrastructure capacity and traffic flow. For these purposes, spatially disaggregated data sets provided by Eurostat such as road density, use intensity, and accessibility indicators enhance strategic planning through the provision of empirical content to support dynamic input by operating systems. Such systems integrated together facilitate enhanced scheduling, reduce peak-time congestion, and avoid infrastructure overload during vulnerable times (Drljača & Sesar, 2023).

2. Less Degradation of Road Infrastructure Through Improved Management of Weight, Speed, and Routing of Heavy Vehicles

Minimizing road wear entails accurate management of freight truck parameters.The OpenTripModel (OTM) again plays a central role by holding the dimensions of vehicles, weight, and compliance data that are critical for controlling access to weight-sensitive infrastructure. TMS and Fleet Management Systems (FMS) cooperate to provide only authorized vehicles to be routed along prescribed corridors. These systems offer real-time surveillance and auto-compensation for weight or speed violations(Shivkumar & Supriya, 2024).As the specialists have put it in the interview, these kinds of systems, as much as they are taken up heterogeneously by hauliers, are the bedrock to implementing dynamic access rules that minimize infrastructure damage.

3. Realizing Climate Objectives by Reducing Congestion and Prioritizing Climate-Friendly Vehicles

IA plays a major role in achieving environmental goals through low-emission zone enforcement and congestion reduction. Standards like OTM, G2B, and B2G allow regulatory bodies to share access criteria (e.g., emission limits) with fleet operators in digital formats(Lange et al., 2022). These regulations help in providing priority to low-emission or electric vehicles. TMS, FMS, and TAS combine to select green routes and schedule deliveries during off-peak hours and thereby check emissions and congestion(Drljača & Sesar, 2023).Apart from these operational facilitators, Eurostat monitors road transport emissions and modal split, and National Access Points (NAPs) disperse real-time information regarding congestion levels and emission zone borders.These data flows, made interoperable, allow for optimal routing that aligns with environmental policy and digital access restrictions.Experts in interviews pointed out the necessity of combining these data flows in policy-based transport access, especially in urban freight corridors.

4. Increasing Road Safety Through Less Overloading or Improved Insight Into Safety Incidents

Improving road safety depends on monitoring vehicle compliance and detecting high-risk behavior in real time. Standards such as OTM, G2B, and B2G enable the digital communication of vehicle permits, load information, and incident alerts(Lange et al., 2022). FMS and TMS provide the means to receive information and respond to it through route adjustment, load rebalancing, or speed adjustment(Drljača & Sesar, 2023).NAPs also contribute by providing Safety-Related Traffic Information (SRTI), e.g., alerts pertaining to congestion, road hazard, and abnormal vehicle behavior, and hence enhancing real-time situational awareness for operators and authorities alike.As the interviewees described, real-time coupling with FMS and infrastructure systems allows the operators to respond on time to hazardous conditions, thereby directly contributing to IA’s safety goals.

5. Creation of a Level Playing Field Between Different Hauliers/Carriers and Improving Compliance

Transparency and compliance in today's IA systems rely on secure infrastructure and standardized communication standards. G2B, B2G, and OpenTripModel (OTM) standards enable access on an

equal footing to regulatory information(Lange et al., 2022).Port Community Systems (PCS) and Truck Appointment Systems (TAS) platforms enable open scheduling and documentation(Ericsson & Svensson, 2022). Zero Trust Architecture (ZTA) requires robust identity verification, with access to sensitive data given only to approved users and systems(Kulkarni & Cheikhrouhou, 2024). At the same time, AWS Managed Services (AMS) provides secure and scalable cloud hosting for such systems so that small hauliers can meet expectations without incurring the cost of proprietary infrastructure(Amazon Web Services, Inc., 2025). Interviewees as they noted, this technological foundation is necessary to enable all stakeholders of any scale to play by the same digital rules of governance.

6. Improved Control of the Transport of Abnormal Loads and Dangerous Goods

IA enhances management of abnormal and hazardous transport via checks of vehicle dimensions, permits, and routing. OTM, RFID, and AutoTrix standards ensure timely identification of hazardous transport movement. TMS and FMS provide routing, compliance verification, and warning(Drljača & Sesar, 2023). ZTA checks all system interactions and isolates them, with no unauthorized access being feasible to hazardous cargo data(Kulkarni & Cheikhrouhou, 2024). These platforms are typically hosted on AMS, which offers compliance-enabled cloud services with monitoring, encryption, and access control integrated(Amazon Web Services, Inc., 2025). To facilitate additional digital planning, Eurostat provides harmonized statistics on heavy freight flows and types of road infrastructure, which allows for the prediction of infrastructure bottleneck locations when transporting abnormal loads.As interview specialists put it, it is secure hosting coupled with real-time visibility that holds the key to ensuring safe and legally compliant hazardous goods logistics operations.

7. Controlled Introduction of High Capacity Vehicles

Controlled access of HCVs to road networks is offered by systems that ensure infrastructure compatibility and route permission. Standards like G2B, B2G, and permit systems like AutoTrix enable authorities to make decisions on whether an HCV should be allowed access to a given corridor(Lange et al., 2022). Route planning and tracking of vehicles are made easy by TMS and FMS(Drljača & Sesar, 2023). ZTA is central to managing identity-based control of road network permissions to enable permission for compliant operators and vehicles to access routes(Kulkarni & Cheikhrouhou, 2024). AMS provides such applications with cloud-based resilience and adaptability to meet the demand for managing growth in access data and regulatory communication(Amazon Web Services, Inc., 2025).

8. Faster and More Unified Processing of Transport Documents in Cross-Border Digitalization

Digitalisation of IA is converting paper-based transport operations into real-time system-to-system data exchange across systems like PCS, ERP, and TOS. Technologies such as EDI and RFID facilitate structured data exchange among hauliers, customs, and terminal operators(Imburgia, 2006). Such systems are being made available through AMS, facilitating document handling with high availability and data storage security. ZTA facilitates authentication of all participants in a cross-border transport transaction and least-privilege access to doc systems, removing risk and ensuring compliance(Amazon Web Services, Inc., 2025). National Access Points (NAPs) facilitate such digitalisation by making harmonised metadata on transport restrictions, terminal facilities, and routing regulations available, facilitating interoperability between Member States. Coupled with Eurostat's cross-border logistics indicators, such mechanisms facilitate the achievement of integrated, paperless freight corridors.As evident from the theory and witnessed through interviews, such a shift makes border crossing times shorter and more effective.

6.2 Future Scenarios(5-10 years)

Frameworks	Better use of existing infrastructure with traffic management based on time and place;	Less degradation of road infrastructure through improved management of weight, speed and routing of heavy vehicles;	Realizing climate objectives by reducing congestion and prioritizing climate-friendly vehicles, for example management of low emission zones, and this will give more transparent and greener logistics;	Increasing road safety through, for example, less overloading or improved insight into where safety incidents arise on the road network;	Creation of a level playing field between different haulers/carriers, improving compliance by haulers/carriers with regulations as set out by NRAs;	Improved control of the transport of abnormal loads and dangerous goods;	Controlled introduction of High Capacity Vehicles;	Faster and more unified and controlled processing of transport documents in cross-border transport through digitalization.
Information standards	Datex II	Datex II	Datex II	Datex II	eFTI	eFTI,Datex II	Datex II	eFTI,eCMR
Information systems	Geofencing,I2V, V2I	Geofencing,I2V, V2I	Geofencing,I2V, V2I	V2V,I2V,V2I	Blockchain	Geofencing,I2V, V2I	Geofencing,I2V, V2I	Blockchain
Information security				JWS	AMS,JWS,GDPR, NIS2, Blockchain	AMS,JWS, Blockchain		AMS,JWS,GDPR, NIS2, Blockchain

Fig. 4 Future Scenario for intelligent access(5-10 years)

1. Better Use of Existing Infrastructure with Traffic Management Based on Time and Place
In the future scenario, Datex II and vehicle-infrastructure communication systems like Geofencing, I2V, and V2I will be central to managing infrastructure access based on time and location(Dey et al., 2016). Datex II provides standardized, real-time traffic and event data, enabling infrastructure operators to communicate digital access permissions dynamically. These systems, when integrated, will allow authorities to grant or restrict access based on road usage patterns, time windows, and vehicle characteristics. JSON Web Signatures (JWS) will ensure that data exchanged between vehicles and infrastructure remains secure and verifiable. These advancements will support intelligent routing and efficient infrastructure use, especially in congested or time-restricted zones.

2. Less Degradation of Road Infrastructure Through Improved Management of Weight, Speed, and Routing of Heavy Vehicles
To minimize infrastructure wear, future IA systems will rely on Datex II, combined with Geofencing, I2V, and V2I systems, to dynamically enforce restrictions based on vehicle weight, dimensions, and speed. These technologies will allow for conditional access based on real-time vehicle telemetry and road condition data (Guercini, Lind, & Melander, 2022). JWS will authenticate access-related data, ensuring its integrity for infrastructure planning and compliance enforcement. These tools will make it possible to redirect overweight vehicles or deny access during vulnerable conditions, thus preserving critical road assets.

3. Realizing Climate Objectives by Reducing Congestion and Prioritizing Climate-Friendly Vehicles
Future IA will contribute significantly to climate goals through Datex II and connected systems like Geofencing, I2V, and V2I, which enable real-time management of access to low-emission zones. These tools will allow authorities to prioritize or restrict access based on vehicle emission class or

environmental impact. Vehicles can receive access decisions instantly via I2V messages, improving flow and compliance. JWS will protect this sensitive data, ensuring only authorized entities exchange access-related credentials. This will lead to greener, more transparent logistics, especially in urban areas (Lindkvist, Lind, & Melander, 2023).

4. Increasing Road Safety Through Less Overloading or Improved Insight into Safety Incidents
Improving road safety in future IA will depend on vehicle-to-infrastructure and vehicle-to-vehicle systems (V2V, I2V, V2I) that enable proactive monitoring and control. These systems will communicate real-time safety-critical information such as overloading alerts, sudden braking, or crash risks. Datex II will serve as the data standard for reporting and processing traffic events. JWS will secure these transmissions, ensuring data cannot be tampered with. Together, these tools will help transport authorities and fleet operators prevent accidents and optimize emergency responses (Dey et al., 2016; Pathak & Shrawankar, 2009).

5. Creation of a Level Playing Field Between Different Hauliers/Carriers and Improving Compliance
In the future, equitable access will be enforced through digital frameworks like eFTI, supported by tamper-proof standards such as Blockchain. These allow hauliers to prove compliance digitally. AWS Managed Services (AMS) will host these platforms securely, ensuring regulatory compliance and availability(Amazon Web Services, Inc., 2025). ZTA will govern how each actor accesses the data, enforcing identity verification and segmentation. This dual setup guarantees that all operators, regardless of their size, follow the same access protocols. Interviewees emphasized that a mix of open standards and strict, cloud-based identity control is key to a transparent IA ecosystem.

6. Improved Control of the Transport of Abnormal Loads and Dangerous Goods
In future IA, Datex II and eFTI will structure data exchange, while Geofencing, I2V, and V2I systems will monitor and enforce compliance in real time (Dey et al., 2016; Pathak & Shrawankar, 2009). Blockchain will provide immutable verification of permits and cargo types. AMS will support these services in a compliant cloud environment, while ZTA ensures that only verified users or systems—e.g., an authorized customs officer or gate terminal—can access or update transport data. This layered control improves the safety, traceability, and legal defensibility of IA operations for abnormal and hazardous loads (Dasaklis et al., 2024).

7. Controlled Introduction of High Capacity Vehicles
For HCVs, IA will require real-time infrastructure awareness, enabled by Datex II, Geofencing, and V2I systems. These will dynamically grant or deny access based on road readiness, vehicle configuration, and traffic patterns. (Dey et al., 2016; Pathak & Shrawankar, 2009). ZTA will manage segmented access control for users and vehicles across the digital infrastructure, while AMS provides scalable, high-availability hosting for data-intensive systems(Amazon Web Services, Inc., 2025).This ensures both security and performance for jurisdictions integrating HCVs.

8. Faster and More Unified Processing of Transport Documents in Cross-Border Digitalization
In the future, transport documents like eFTI and eCMR will be exchanged seamlessly through platforms hosted on AWS Managed Services, enabling secure, scalable operations(Dasaklis et al., 2024). Blockchain will verify authenticity, and ZTA will ensure that access to transport data—by border agents, hauliers, or terminals—is governed by verified identity and role-based permissions. Together, these systems reduce the time, risk, and cost of international freight movements(Kulkarni &

Cheikhrouhou, 2024).. As noted by experts in the interview, such trust-based, secure architectures will be essential to the success of digital cross-border freight.

6.3 Other Thoughts

Mindset of Truck Operators and the Human Factor

Another strand that emerged time and again in the expert interviews was the mindset of truck drivers, particularly independent hauliers and small ones, which inclines to perceive digitalization as a regulation instead of an added value. Operators tend to be slow in adopting digital platforms such as Truck Appointment Systems (TAS) or Port Community Systems (PCS) due to concerns regarding privacy over the data, the complexity of the systems in their eyes, and concern for increased surveillance. This is representative of a larger problem of digitalization in logistics: technology is not the constraint but human adoption. While large logistics firms with in-house specialist IT teams embrace digital scheduling, geofencing, and live permit systems, it is less easy for the smaller operators to be able to afford or appreciate the digital literacy, technical support, or economic incentive to comply. This deficit jeopardizes inclusive IA system deployment on EU-wide and national networks.

Organizational Readiness and Fragmentation

Even in the presence of such standards as eFTI and eCMR, organisational fragmentation is a major stumbling block in making IA seamless. Several ports, motorways authority, and logists operate across disparate heterogeneous systems at different stages of integration.For example, a terminal could have automated gate services and DATEX II data feeds but, for example, downstream or upstream counterparts could still be using manual documentations or email-based appointments. This maturity asymmetry in the digital realm constrains the optimal realization of IA benefits such as dynamic slot allocation, time-based access control, and coordinated security enforcement.

Moreover, the majority of logistics firms lack a general digital strategy or do not attribute ownership to access data governance, so it is difficult to synchronize IA initiatives with overall supply chain goals. This is compounded by short-term ROI demands, where investment in access platforms is generally quantified by throughput or efficiency gains alone without regard to long-term benefits like reduced emissions, regulatory compliance, or employee health.

Trust and Data Sovereignty

Another major consideration is the issue of digital trust and data sovereignty. The operators are concerned with who owns and controls the access data they generate particularly in cross-border contexts where the application of GDPR is patchy. The truckers and small businesses in the interviews also complained about monitoring, abuse of data, and lack of transparency regarding how their driving behavior, load data, or access history could be used by regulators or competitors. The lack of an open, accountable data governance framework makes it harder to build trust and a willingness to share data across the logistics value chain. For IA to succeed at scale, digital trust must be built not only through security architectures like Zero Trust Architecture (ZTA), but also policy interventions that ensure accountability, redress, and informed consent.

Inclusiveness and Policy Support

Finally, a major area of contention is inclusive IA policy regimes that exclude no small players. Policy support in the guise of digital tool subsidies, standardization rules, and driver training programs can democratize access to IA systems. While innovation in technology is picking up pace through AI-based fleet optimization, blockchain-secured access records, and access rules adaptive to behavior policy and learning must catch up. If left unchecked, the digital divide will deepen, reinforcing disparities in access to functioning infrastructure and compliance with regulation.

7. Conclusion

7.1 Purpose

The general purpose of this research is to investigate contemporary and future aspects of information standards, information systems and information security to achieve IA for road freight transportation and port-terminal logistics. As road and sea logistics become increasingly complex at the interface, the study sought to understand how digital technologies might be strategically adopted in order for the right vehicle, carrying the right load, on the right road, at the right time, to make optimal use of infrastructure, improve security, and reduce congestion. The objective was to present a comprehensive review of existing implementations and emerging developments in IA with a focus on their interoperability, compliance, and electronic governance.

7.2 Process

The research used a qualitative, exploratory research methodology grounded in a combination of literature review, expert interviews, and empirical analysis. The literature review engaged with intelligent transport systems, port digitalization, and new generation logistics information technologies. Eight interviews were conducted with stakeholders from logistics companies, infrastructure organizations, and digital platform providers. The interviews were instrumental in developing useful challenges and success factors for the implementation of IA technologies. The results were analyzed and correlated to eight impact areas derived from the CEDR ISAC framework, i.e., usage of infrastructure, road wear, climate targets, safety, justice, handling abnormal loads, integration of high-capacity vehicles (HCV), and cross-border digitalization.

7.3 Main Findings

Fragmentation and Asymmetry in Adoption

One of the most important findings is the significant disparity in the extent of digital maturity between players within logistics. Terminal operators and larger players within logistics have started to invest in IA-enabling systems such as TAS, TMS, and PCS, but there are still plenty of SMEs excluded due to high cost, lack of availability of IT professionals, or absence of interoperability. Several interviewees termed this "digital divide" as an actual hindrance toward the mass deployment of IA.

Partial Implementation of Information Standards

Electronic standards such as eFTI and eCMR are being rolled out at the pilot level, particularly for cross-border freight and customs clearance. However, interviewees confirmed that full compliance is still weak and practical implementation is still patchy between and within countries, and between terminals. The eFTI rule will be more impactful after 2026, but already there remain a number of players still using non-integrated electronic or paper-based systems.

The systems work in Isolated platforms

Port Community System (PCS) and Truck Appointment System (TAS) are being used for terminal gate administration and scheduling but typically operating within closed systems. It was emphasized by the experts that the interface from the outside systems like ERP or FMS is limited, which causes duplication of data and inefficient administration. Only a small number of advanced ports have developed full platform interoperability to allow real-time gate usage decisions based on live cargo and vehicle data.

Security is an Increasing Priority, but For Now, an Afterthought

While information security has been recognized as a priority especially from the viewpoint of the GDPR and NIS2 directives, respondents showed that security is only dealt with reactively, and never

proactively, by the majority of logistic operators, except for large operators. Security systems like Zero Trust Architecture (ZTA) and AWS Managed Services (AMS) are neither being utilized in practice except for large players. This implementation gap poses the risk of data breaches, especially as systems get more interconnected.

Outstanding Opportunity for Use of Real-Time Data, but Traditionally Underutilized

Access, based on high-potential real-time, criteria-based IA, is delivered by technologies like OpenTripModel (OTM), DATEX II, and telematics for vehicles. However, they are theoretical or pilot-scale when it comes to deployment. The responses mentioned that, though dynamically varying access based on weights, emissions, or compliance is technically achievable, it is not typically done for operational purposes. Access is still typically timetable-based or through manual gate checks.

Institutional and Regulatory Misalignment

Several interviewees cited the lack of regulatory harmonization between member states as one major hindrance. For instance, an eCMR-compatible shipment may clear one border but will not clear another. Similarly, there are regulations for high-capacity vehicles or emissions taxes which vary across areas, and solutions for IA don't scale conveniently across networks. This generates inefficiencies for broader deployment of secure and interoperable logistic systems.

Operational Benefits When Implemented

Wherever the IA systems are being used, for example, advanced harbors within Europe, already established through experience, have shorter turnaround times, better flow of vehicles, and increased reliability of operations on access. A 17% reduction in the truck turnaround time was realized according to one interviewee after implementation of TAS and gate system automation. Such benefits confirm the operational feasibility for use when systems integrate well and backed by clear digital rules and infrastructure preparedness.

Highlighted Good Examples of eFTI and eCMR

This research has identified strong, practical examples of eFTI and eCMR that validate their practical use and scalability. Whether the open-source eFTI solution in Germany and national PoC of Finland, or Bolk Transport's end-to-end operating model and Spain's legislative push toward compulsory digital consignment notes, these instances validate the frameworks' ability for driving transformational change toward intelligent access. A detailed analysis and reference links are listed in Appendix B.

7.4 Theoretical and Practical Contributions

The study offers a theoretical model of IA through the integration of digital governance theory, smart port planning, and the CEDR's IA model into a single comprehensive explanation of existing and future logistics ecosystems. It substantiates the hypothesis that IA not only optimizes the process but also maximizes regulation and sustainability objectives by offering access control based on criteria in real time.

In operational terms, the research provides a strategic blueprint for policymakers and logistics providers. By overlaying standards, systems, and security tools onto eight IA benefit areas, it creates a decision-support framework capable of guiding investment, regulatory planning, and infrastructure planning. Terminals can order TAS and PCS adoption by priority based on these findings, and road authorities can order geofencing, V2I systems, and secure digital permit exchange platforms.

7.5 Future Research

Empirical data for operational impacts of Intelligent Access (IA) roll-outs at freight terminals and transport corridors is an important research direction for the future. It is qualitatively reported that systems such as Truck Appointment Systems (TAS) and Port Community Systems (PCS) reduce waiting and congestion, but quantitative evidence for emissions, lead times, or for more efficient use

of infrastructure is limited. Longitudinal studies can compare before-and-after key metrics for the roll-out of systems, and provide evidence for large-scale policy take-up. Particular care must be given to assessing the impact of standards such as eFTI and eCMR, which will be made mandatory within a few years under EU legislation. Their impact on administrative ease, customs clearance time, and cross-border compliance must be validated on the basis of real-life case data, focusing on high-traffic logistic corridors.

One important path for future studies is integrating the digital environment for IA with small and medium-sized enterprises (SMEs). As we highlighted through interviews with experts, SMEs don't have the capacity to apply leading-edge information systems or follow evolving digital standards due to limited technical knowledge and economic resources. Future studies can focus on the use of low-threshold solutions or intuitive modules for digital accessibility, for example, app-based user interfaces or plug-and-play APIs based on OpenTripModel (OTM) architecture. Supportability studies for the same through public funding, regulatory sandbox, or subsidizing for interoperability can create equity for accessibility and policy compliance irrespective of scales for logistics players.

Additionally, future research must address organizational and behavioral challenges for deploying IA, i.e., for drivers and dispatchers. Attitudes for drivers, comfort and familiarity with digital systems, justice and surveillance perceptions must be investigated to avoid resistance and non-uptake. Field studies using ethnography or behavioral design can be used to obtain insight into the use of access control systems, e.g., geofencing alarms, autonomous gate systems, or V2I messages, and whether, and under what circumstances, the technology has an effect and to what extent it has an effect on job satisfaction, safety attitude, or perceived tension. A people-first strategy must be used to make IA systems effective and socially acceptable and be reliable in the eyes of end users.

In addition, there is growing demand for research into cross-border technical compatibility and regulatory harmonization in the context of IA. While frameworks like eFTI and DATEX II provide a framework for standardized data transfer, day-to-day implementation is undermined by technological readiness, national regulations, and digital readiness. Regulatory sandboxes or pilot regions, where freight carriers can use a harmonized set of digital documents, geofencing rules, and enforcement systems across borders, can be envisioned and tried out through further studies. The role played by the European National Access Points (NAPs) to enable standardized access governance and secure data transmission between jurisdictions can be addressed by the studies as well.

Security and compliance frameworks are also an important field for future research. As more interconnected IA systems are being used, they are under threat of cyber attack, data breaches, and misuse. As a result, research must study the implementation of Zero Trust Architecture (ZTA) and Amazon Web Services' Managed Services (AMS) within logistics environments to safeguard sensitive data such as shipment manifests, route permits, and real-time telemetry data from vehicles. More cutting-edge topics like intrusion detection by using AI, secure cloud hosting, and biometric authentication verification within IA systems are worth studying. Blockchain technologies must also be explored further for use within processing anomalous load permits, vehicle histories, and compliance logs. With its tamper-proof, verifiable chain, blockchain can be an important element to facilitate trust and audibility within decentralized IA systems.

Last but not least, the lawfulness and ethics of using algorithmic and AI-based decision-making tools for making access decisions must be examined critically by forthcoming research. As IA systems are currently deploying artificial intelligence for real-time direction, permit screening, and risk

assessment, issues relating to algorithmic transparency, explainability, and the right to explain start making headlines. Research must study how the GDPR and incoming regulatory requirements for AI can be mapped onto IA systems for enabling lawful, fair, and explainable decision-making. A cross-disciplinary research agenda involving logistics technology, data protection law, and AI ethics is now overdue for enabling IA systems to develop responsibly and inclusive.

8. References

Adams, W. C. (2015). Conducting semi-structured interviews. In K. E. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), Handbook of Practical Program Evaluation (4th ed., pp. 492–505). Jossey-Bass.

Aifantopoulou, G., Mylonas, C., Dolianitis, A., Stamelou, A., Psonis, V., & Mitsakis, E. (2020). National Access Points for Intelligent Transport Systems Data: From Conceptualization to Benefits Recognition and Exploitation. Retrieved from https://arxiv.org/abs/2010.12036

Alaskari, O., Pinedo-Cuenca, R., & Ahmad, M. M. (2021). Framework for implementation of Enterprise Resource Planning (ERP) systems in Small and Medium Enterprises (SMEs): A case study. *Procedia Manufacturing*, *55*, 424–430. https://doi.org/10.1016/j.promfg.2021.10.058

Amazon Web Services, Inc. (2025). AMS Advanced User Guide: AMS Advanced Concepts and Procedures. Retrieved from https://docs.aws.amazon.com/managedservices/latest/userguide/

Aremu, A. Y., Shahzad, A., & Hassan, S. (2018). Determinants of Enterprise Resource Planning Adoption on Organizations' Performance Among Medium Enterprises. *LogForum*, *14*(2), 245–255. https://doi.org/10.17270/J.LOG.2018.277

Aventeon. (2023). *Open Trip Model (OTM) is a practical solution that has been successfully implemented by Aventeon*. Retrieved from https://www.aventeon.com/blog/open-trip-model-otm-is-a-practical-solution-that-has-been-successfully-implemented-by-aventeon

Bakhtina, M., Matulevičius, R., & Malina, L. (2024). Information Security and Privacy Management in Intelligent Transportation Systems. Complex Systems Informatics and Modeling Quarterly, 38, 100–131.

Bauk, S., Schmeink, A., & Colomer, J. (2018). An RFID model for improving workers' safety at the seaport in transitional environment. Transport, 33(2), 353–363. https://doi.org/10.3846/16484142.2016.1233512

Bryman, A. (2016). *Social Research Methods* (5th ed.). Oxford University Press.

CEDR ISAC. (2024). *Cybersecurity and Data Governance Guidelines for Road Authorities*. Conference of European Directors of Roads.

Challa, A. (2016). *Fleet Management System*. Kansas State University. Retrieved from https://core.ac.uk/display/77979434

Choi, H. R., Kim, H. S., Park, B. J., Park, N. K., & Lee, S. W. (2003). An ERP approach for container terminal operating systems. *Maritime Policy & Management*, 30(3), 197–210. https://doi.org/10.1080/0308883032000089549

Chountalas, P., Michalopoulos, V., & Sdogos, C. (2024). The Adoption of eCMR in European Logistics: Barriers and Opportunities. *Transportation Research Procedia*, 72, 165–174.

Croma Campus. (2024, November 11). What to expect from AWS in 2025: The future of cloud computing? AWS Community.

https://community.aws/content/2ohL4IXtdRmiFsnF8eugv9IIpAA/what-to-expect-from-aws-in-2025-the-future-of-cloud-computing?lang=en

Dean, M. (2022). Multi-criteria decision-making in sustainable infrastructure planning. Journal of Infrastructure Systems, 28(1), 04021045.

Delgado, A. M., Samper-Zapater, J. J., Del Campo, S., Martínez Durá, J. J., Rocha, J. M., & Garcia Calderaro, J. F. (2024). *Evolution of DATEX II Standard towards Open Data: A Case Study on LOD-RoadTran18 project*. In *12th Euro American Conference on Telematics and Information Systems (EATIS 2024)* (pp. 1–4). ACM. https://doi.org/10.1145/3685243.3685292

Dasaklis, T. K., Casino, F., & Patsakis, C. (2024). A Blockchain-Based Framework for Secure Cargo Handling in Port Logistics. *Computers & Industrial Engineering*, 179, 108012. https://doi.org/10.1016/j.cie.2023.108012

DATEX II. (n.d.-a). *About DATEX II*. Retrieved May 10, 2025, from https://datex2.eu/about/

DATEX II. (n.d.-b). *Specifications*. Retrieved May 10, 2025, from https://datex2.eu/specifications/

DATEX II. (n.d.-c). *ITS Directive and EU Compliance*. Retrieved May 10, 2025, from https://datex2.eu/its-directive/

Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation. Transportation Research Part C: Emerging Technologies, 68, 168-184. https://doi.org/10.1016/j.trc.2016.03.008

Dijkstra, L., Poelman, H., & Ackermans, L. (2019). *Road transport performance in Europe: Introducing a new accessibility framework*. European Commission, Directorate-General for Regional and Urban Policy.

Dorofeev, A., Altukhova, N., Filippova, N., Pashkova, T., & Ponomarev, M. (2020). Development of Transportation Management System with the Use of Ontological and Architectural Approaches to Ensure Trucking Reliability. Sustainability, 12(20), 8504. https://doi.org/10.3390/su12208504

Drljača, M., & Sesar, V. (2023). Supply chain transportation management. Transportation Research Procedia, 74, 338–345. https://doi.org/10.1016/j.trpro.2023.11.153

Ebirim, G. U., Unigwe, I. F., Asuzu, O. F., Odonkor, B., Oshioste, E. E., & Okoli, U. I. (2024). A critical review of ERP systems implementation in multinational corporations: Trends, challenges, and future directions. *International Journal of Management & Entrepreneurship Research*, *6*(2), 281–295. https://doi.org/10.51594/ijmer.v6i2.770

EPRS – European Parliamentary Research Service. (2021). Review of the Intelligent Transport Systems Directive. PE 694.240. Retrieved from https://www.europarl.europa.eu

Ericsson, R., & Svensson, P. (2022). *Drivers and barriers for truck appointment systems at container terminals: A business model perspective* [Master's thesis, Chalmers University of Technology]. Chalmers Publication Library.

European Commission. (2024). MMTIS Implementation Handbook: Commission Delegated Regulation (EU) 2017/1926 (as amended by 2024/490). Directorate-General for Mobility & Transport.

European Commission. (2024). National Access Points: A Mechanism for Accessing, Exchanging and Reusing Transport-Related Data under Delegated Acts of the ITS Directive (2010/40/EU). Retrieved from https://transport.ec.europa.eu

European Commission. (2020). *Regulation (EU) 2020/1056 on Electronic Freight Transport Information (eFTI)*. Official Journal of the European Union.

European Commission. (2020). *Sustainable and Smart Mobility Strategy – putting European transport on track for the future*. Brussels: European Commission.

European Commission. (2010). *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010L0040-20231220

Eurostat. (2000). *Special Feature on Road Transport Statistics*. Luxembourg: Publications Office of the European Union.

Eurostat. (2022). *Key Figures on European Transport – 2022 Edition*. Publications Office of the European Union.

Flick, U. (2014). An Introduction to Qualitative Research (5th ed.). SAGE Publications

Hasan, S. F., Siddique, N., & Chakraborty, S. (2013). Intelligent Transport Systems: 802.11-based Roadside-to-Vehicle Communications. Springer Science & Business Media.

Hassan, H., Wolshon, B., & Sultana, T. (2023). Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) Passenger and Freight Vehicle Applications to Enhance Safety and Efficiency in Coastal Evacuations (Final Research Report). Maritime Transportation Research and Education Center, Louisiana State University.

Heikkilä, M., Saarni, J., & Saurama, A. (2022). Innovation in Smart Ports: Future Directions of Digitalization in Container Ports. *Journal of Marine Science and Engineering, 10*(1925). https://doi.org/10.3390/jmse10121925

Heilig, L., & Voß, S. (2016). Information systems in seaports: A categorization and overview. Information Technology and Management, 18(2), 179–201. https://doi.org/10.1007/s10799-016-0269-1

Heilig, L., & Voß, S. (2017). Information systems in seaports: A categorization and overview. Information Technology and Management, 18(3), 179–201. https://doi.org/10.1007/s10799-016-0269-1

Hemeleers, R. (2023). *How e-CMR and eFTI Work Together in an EU Federated Data Sharing Architecture*. EU Data Logistics Festival, Brussels.

Hendriks, L., Jorna, R., Barr, J., & Lubrich, P. (2018). National Access Points: Challenges for Success. 25th ITS World Congress, Copenhagen. Retrieved from https://www.its-platform.eu

Im, H., Yu, J., & Lee, C. (2021). Truck Appointment System for Cooperation between the Transport Companies and the Terminal Operator at Container Terminals. *Applied Sciences, 11*(1), 168. https://doi.org/10.3390/app11010168

Imburgia, M. J. (2006). The role of RFID within EDI: Building a competitive advantage in the supply chain. IEEE.

Inkinen, T., Helminen, R., & Saarikoski, J. (2019). Port digitalization with open data: Challenges, opportunities, and integrations. Journal of Open Innovation: Technology, Market, and Complexity, 5(2), 30. https://doi.org/10.3390/joitmc5020030

Jacobsson, S. (2023). Managing Terminal and Transport Processes with Access Management Services. *Transportation Journal, 62*(2), 144–176. https://doi.org/10.5325/transportationj.62.2.0144

Jacobsson, S. (2019). Potential improvements for access management in intermodal freight terminals: Designing and testing a service for small road haulers. World Review of Intermodal Transportation Research, 8(3), 245–264. https://doi.org/10.1504/WRITR.2019.10023087

Jacobsson, S., Arnäs, P. O., & Stefansson, G. (2017). Access management in intermodal freight transportation: An explorative study of information attributes, actors, resources and activities. Research in Transportation Business & Management, 23, 106–124. https://doi.org/10.1016/j.rtbm.2017.02.012

Jacobsson, S., Arnäs, P. O., & Stefansson, G. (2018). Differentiation of access management services at seaport terminals: Facilitating potential improvements for road hauliers. Journal of Transport Geography, 70, 256–264. https://doi.org/10.1016/j.jtrangeo.2018.06.009

Jacobsson, S., Arnäs, P. O., & Stefansson, G. (2020). Automatic information exchange between interoperable information systems: Potential improvement of access management in a seaport terminal. Research in Transportation Business & Management. https://doi.org/10.1016/j.rtbm.2020.100429

Jacobsson, S., & Lantz, B. (2024). Evaluation of the implementation of automated gate services in a seaport freight terminal. *World Review of Intermodal Transportation Research, 12*(1), 25–43.

Jones, M. B., Bradley, J., & Sakimura, N. (2015). *JSON Web Signature (JWS)*. RFC 7515. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc7515.html

Kłos, S., Jakubowski, J., & Patalas, J. (n.d.). A framework of ERP system evaluation of project-driven enterprise: A case study. *University of Zielona Góra, Department of Mechanical Engineering*.

Komar, K.V. (2024). Information Security in Intelligent Transportation Systems Traffic Management. Conference Paper presented at the International Scientific-Practical Conference on Information Technologies: Theory and Practice, 20–22 March 2024, National University of Life and Environmental Sciences of Ukraine.

Koutsorodi, A. A., Adamopoulou, E. F., Demestichas, K. P., & Theologou, M. E. (2006). Terminal management and intelligent access selection in heterogeneous environments. *Mobile Networks and Applications*, 11(6), 861–871. https://doi.org/10.1007/s11036-006-0054-1

Kulkarni, A. J., & Cheikhrouhou, N. (Eds.). (2024). Intelligent Systems for Smart Cities: Select Proceedings of the 2nd International Conference, ICISA 2023. Springer. https://doi.org/10.1007/978-981-99-6984-5

Kunz, N., Van Wassenhove, L. N., Hov, K., & McConnell, R. (2015). Centralized vehicle leasing in humanitarian fleet management: the UNHCR case. *Journal of Humanitarian Logistics and Supply Chain Management*, 5(2), 228–252. https://doi.org/10.1108/JHLSCM-07-2015-0034

Lange, A.-K., Nellen, N., & Jahn, C. (2022). Truck Appointment Systems – How Can They Be Improved and What Are Their Limits? In *Proceedings of the Hamburg International Conference of Logistics (HICL)* (pp. 617–626).

Ligteringen, H. (2021). *Ports and Terminals*. Delft Academic Press.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Martín-Soberón, A. M., Monfort, A., Sapiña, R., Monterde, N., & Calduch, D. (2014). Automation in port container terminals. *Procedia - Social and Behavioral Sciences, 160*, 195–204. https://doi.org/10.1016/j.sbspro.2014.12.131

Melo-Castillo, A., Bures, P., Herrera-Quintero, L. F., & Banse, K. (2017). *Design and implementation of DATEX II profiles for truck parking systems*. IEEE. https://ieeexplore.ieee.org/document/8102132

Min, H., Ahn, S.-B., Lee, H.-S., & Park, H. (2017). An integrated terminal operating system for enhancing the efficiency of seaport terminal operators. *Maritime Economics & Logistics*, 19(3), 428–450. https://doi.org/10.1057/s41278-017-0069-5

More, N., Dhekane, S., Konde, M., & Sapate, S. D. (2022). Transport Management System. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 358–360. https://doi.org/10.17148/IJARCCE.2022.11464

Mueck, M., & Gaie, C. (Eds.). (2025). *European Digital Regulations*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-80809-8

Mylonas, C., Mitsakis, E., Ayfantopoulou, G., Stavara, M., Tzanis, D., Yannis, G., & Laiou, A. (2023). Harmonization of National Access Points to Intelligent Transport Systems data: A data content and added value perspective. Transportation Research Procedia, 72, 2928–2935. https://doi.org/10.1016/j.trpro.2023.11.839

NAPCORE. (2022). Approach Towards napDCAT-AP Specification v1.0. Report of Guidelines and Best Practices. Retrieved from https://napcore.eu

Notteboom, T., Pallis, A., & Rodrigue, J.-P. (2022). *Port Economics, Management and Policy*. Routledge.

Nykänen, L., Lankinen, M., & Nordström, M. (2024). *Preparation for eFTI Implementation*. Executive Summary, Traficom Research Reports 09/2024.

OpenTripModel.org. (n.d.). *Preface – OpenTripModel Documentation*. Retrieved from https://www.opentripmodel.org/docs/preface
OTM Developer Portal. (2023). *OTM Overview*. Retrieved from https://otm5developerportal.redoc.ly/developer-portal/otm_overview/

Pathak, S. N., & Shrawankar, U. (2009). Infrastructure to Vehicle real Time Secured Communication. Proceedings of 2009 International Symposium on Computing, Communication, and Control, Singapore, 9-11 October.

Patton, M. Q. (2015). Qualitative Research & Evaluation Methods (4th ed.). SAGE Publications.

Perallos, A., Hernandez-Jayo, U., Onieva, E., & García-Zuazola, I. J. (Eds.). (2015). Intelligent Transport Systems: Technologies and Applications. John Wiley & Sons, Inc.

Perego, A., Perotti, S., & Mangiaracina, R. (2021). Electronic consignment notes and digital freight documentation: Implications for transport logistics. Transportation Research Part E: Logistics and Transportation Review, 148, 102269. https://doi.org/10.1016/j.tre.2021.102269

Phan, M.-H., & Kim, K. H. (2016). Collaborative truck scheduling and appointments for trucking companies and container terminals. *Transportation Research Part B: Methodological, 86*, 37–50. https://doi.org/10.1016/j.trb.2016.01.006

Shivkumar, S., & Supriya, M. (2024). A Framework for Fleet Management Using IoT and Predictive Analytics. *15th ICCCNT IEEE Conference*, IIT-Mandi.

Singh, C. (2023). The European approach to cybersecurity in 2023: A review of the changes brought in by the Network and Information Security 2 (NIS2) Directive 2022/2555. *International Company and Commercial Law Review*, 5, 251–261.

Stavropoulos, D., Kazdaridis, G., Korakis, T., Katsaros, D., & Tassiulas, L. (2012). Demonstration of a Vehicle-to-Infrastructure (V2I) communication network featuring heterogeneous sensors and delay-tolerant network capabilities. TridentCom 2012, LNICST 44, 403-405.

Tijan, E., Aksentijević, S., & Čišić, D. (2014). Seaport Cluster Information Systems - A Foundation for Port Community Systems' Architecture. MIPRO 2014.

Tijan, E., Jović, M., Panjako, A., & Žgaljić, D. (2021). The role of port authority in port governance and port community system implementation. Sustainability, 13(5), 2795. https://doi.org/10.3390/su13052795

TRA. (2022). Mobilithek – The National Access Point for Germany. Presented at Transport Research Arena. Retrieved from https://mobilithek.info

Wang, R., & Li, H. (2020). Assessment and optimization of the port logistics data governance capacity based on enhanced MNA-SAA approach. [Preprint]. Nanjing Tech University & Shandong University of Science and Technology.

Wang, J., Liu, J., Wang, F., & Yue, X. (2021). Blockchain technology for port logistics capability: Exclusive or sharing. Transportation Research Part B, 149, 347–392. https://doi.org/10.1016/j.trb.2021.05.010

Williams, B. (2008). Intelligent Transport Systems Standards. Artech House.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems*, 12(1), Article 2. https://doi.org/10.1145/3389685

Zimmerman, P., Küchle, J., Rautmann, S., & Willrodt, S. (2021). *Terminal Operating Systems 2021: An international market review of current software applications for terminal operators*. Fraunhofer Center for Maritime Logistics and Services.

Appendix A-Interview Guide

General

- Small intro asking their names?
- What is your current work position?
- How long have you been working in this position?
- Can you describe your role and responsibilities in your organization?
- How does your work relate to Intelligent Access (IA) in road freight transport and port-terminal logistics?

RQ1. Information Standards, Information Systems, and Information Security in IA

Current (0-1 year) Implementation

- From the following information standards (e.g., eFTI, eCMR, RFID) that we have identified, which ones would you say is currently in use for:
    - Road hauliers?
    - Smart roads (highways and cities)?
    - Smart parking?
    - Terminals and ports?
- From the following information systems (e.g., TMS, FMS, ERP, PCS, TAS) that we have identified, which ones would you say is currently in use for:
    - Road hauliers?
    - Smart roads (highways and cities)?
    - Smart parking?
    - Terminals and ports?
- From the following information security (e.g., AMS, ZTA, RFID) that we have identified, which ones would you say is currently in use for:
    - Road hauliers?
    - Smart roads (highways and cities)?
    - Smart parking?
    - Terminals and ports?
- How effectively do these standards ensure data exchange and compliance across stakeholders?
- One of the standards and systems that have been discussed in previous research is Geofencing, how would you say that it can affect IA??

Future (5-10 years) Expectations

- What new information standards and systems do you expect to emerge for IA in the next 5-10 years? In all these:
    - Road hauliers?
    - Smart roads (highways and cities)?
    - Smart parking?
    - Terminals and ports?
- What infrastructural developments need to be done in order to incorporate these technologies and achieve IA?
- How do you think that emerging technologies, such as AI, machine learning and IoT, may shape future IA?
- Any other thoughts on future IA information standards, information systems and information security

RQ2. Impact of Contemporary and Future Information Standards, Information Systems, and Information Security on IA

Current (0-1 year) Impact

- How do you think that the existing identified information standards, systems and security can affect IA?
- Could you mention some examples of successful IA implementations in road freight transport and/or in terminal and seaport logistics?
- What are your thoughts about any limitations of current identified IA information standards, information systems and information security?
- What role does data security and privacy compliance (e.g., GDPR) play in IA today?

Future (5-10 years) Considerations

- How do you think that the future identified information standards, systems and security can affect IA even further compared to the current identified ones?
- What role do you think that information security and privacy compliance (e.g.,
- GDPR) will play in IA in the future?
- What security risks do you foresee as IA becomes more digital and automated?
- Any other thoughts on how future information standards, systems and information security may affect IA?
- From the list of potential effects of IA, which of them do you think would be affected by the contemporary and the future frameworks, respectively?

Final Thoughts

- Do you know or are you currently working on any ongoing research activities that could support the development of Intelligent Access (IA) for road freight transport and port-terminal logistics?
- Do you have any planned future research activities related to IA, information standards, information systems, or information security?
- What are the key challenges and opportunities in implementing IA today?
- How do you see the role of digitalization, automation, and security in IA?
- Any other relevant thoughts on this area?
- In what ways do you think your activities contribute to IA development?
- Do you have any recommendations for further research or development in IA?
- Any other insights you'd like to share?

WP3 - Contemporary scenario (0-1 year)

	Road hauliers	Smart roads: Highways	Smart parking	Smart roads: Cities	Terminals / Ports
					
Information standards / systems	e-FTI, e-CMR, TMS, FMS, ERP, B2B	G2B, B2G, V2I, I2V, AutoTRIX (Geofencing)	WIP	G2B, B2G, V2I, I2V, AutoTRIX (Geofencing)	PCS, TAS, B2B, RFID
Information security	WIP	WIP	WIP	WIP	WIP

WP3 - Future scenario (5-10 years)

	Road hauliers	Smart roads: Highways	Smart parking	Smart roads: Cities	Terminals / Ports
					
Information standards / systems	WIP	WIP, AutoTRIX (Geofencing, ???)	WIP	WIP	WIP
Information security	WIP	WIP	WIP	WIP	WIP

Appendix B – Reference Table of eFTI and eCMR Case Examples

Project/Entity	Description	Link
Italy – Gruber Logistics eCMR Pilot	Cross-border pilot using eCMR for pharmaceuticals	https://efti4eu.eu
Open Logistics Foundation – eCMR Lighthouse Project	Over 150 real-life shipments tested for open-source eCMR interoperability	https://openlogisticsfoundation.org
Eurasian Economic Union – eCMR Pilot	eCMR tested across EAEU countries for international document exchange	https://eec.eaeunion.org/en/news/…
Netherlands – Bolk Transport	Integrated eCMR with TransFollow; participated in Dutch IA pilot	https://www.transfollow.org/bolk-transport-and-the-digital-consignment-note/
Netherlands – Smart Multimodal Operations Platform	eFTI-aligned digital freight data exchange under EU4Digital	https://eufordigital.eu/…
Germany – eFTI4EU Pilot	Open-source eFTI platform and eCMR integration with Authority Access Point	https://efti4eu.eu/efti4eu-pilots/pilot-germany
Finland – eFTI Gate Proof of Concept	National PoC including access interfaces by Traficom	https://efti4eu.eu/wp-content/uploads/2024/12/Preparation-for-eFTI-implementation…

Western Balkans – eFTI Roadmap	Regional coordination for eFTI deployment under Transport Community	https://www.transport-community.org/..
Spain – Sustainable Mobility Law	Legislative move toward mandatory eCMR for all road freight	https://www.fieldeas.com/en/ecmr-mandatory