Received 9 February 2021; accepted 9 March 2021. Date of publication 18 March 2021;
date of current version 16 April 2021. The review of this article was arranged by Associate Editor Yongdong Wu.

Digital Object Identifier 10.1109/OJVT.2021.3067209

Securing Seaport Logistic Vehicles Using a Distributed Ledger-Based Credential Management System

ANDREA TESEI [1,2], DOMENICO LATTUCA [1,2], ALEXANDR TARDO [2], LUCA DI MAURO [2], PAOLO PAGANO [2], MARCO LUISE [1], PAULO C. BARTOLOMEU [3], AND JOAQUIM FERREIRA [4]

[1] Dipartimento di Ingegneria dell'Informazione, University of Pisa, 56122 Pisa, Italy
[2] Photonic Networks Technologies National Laboratory, National Inter-university Consortium for Telecommunication (CNIT), 56124 Pisa, Italy
[3] Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[4] Instituto de Telecomunicações, Águeda School of Technology and Management, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

CORRESPONDING AUTHOR: ANDREA TESEI (e-mail: andrea.tesei@phd.unipi.it)

This work was supported by the European Union's Horizon 2020 research, and innovation programme under Grant 768994, also referred as COREALIS (Capacity with a pOsitive enviRonmEntal, and societAL footprInt: portS in the future era).

ABSTRACT Major maritime carriers are globally demanding improvements in the efficiency of port operations. Cargo carried by ships must be loaded and unloaded quickly with minimal stopover time in the port. This requirement mandates seaports to deploy cutting-edge technology to the port area so that logistic processes are increasingly efficient and reliable. In this scenario, the attack surface of such critical infrastructure is growing very rapidly and advanced security techniques must be deployed to enforce a high attack resilience. A Distributed Ledger-based Credential Management System exploiting a Distributed Ledger Technology (DLT) to enable transparent and real-time tracking of logistic vehicles and cargos within a terminal is presented in this paper. Based on a customization of Vehicular Ad-Hoc Network (VANET) security standards, the proposed scheme provides authentication, authorization, and revocation capabilities to promptly exclude misbehaving logistic vehicles from the system, while maintaining an immutable record of all the logistic vehicles' activity. The laboratory validation demonstrates that the delay of the devised scheme is not dependent on the quay area capacity, thus being applicable in seaports of any size. Furthermore, the effectiveness of the solution is demonstrated with the field trial results obtained with the EU Horizon 2020 COREALIS project testbed deployed in the Port of Livorno.

INDEX TERMS Distributed ledger technology, logistic vehicles security, vehicular public key infrastructure, vehicular *ad-hoc* networks (VANETs).

I. INTRODUCTION

The port industry is rapidly evolving to cope with the demand from global maritime carriers. Efficient and digital ports are essential to effectively respond to this demand and the corresponding requirements (e.g. growing transport volumes, environmental restrictions, port competition, etc.). Furthermore, to assure that seaports can handle the increasing throughput demand, several aspects also need to be considered, including cost efficiency, physical and technical infrastructure (e.g. terminal infrastructure and equipment), geographical location, inland transport services (e.g. truck, rail), and secure information and communication technologies (e.g. port community system, terminal operating system) [3]. Moreover, in this sustainable growth scenario, the port surrounding areas must be taken into consideration. Even if efficient ports are vital to the economic and societal development, goods handling in the port (e.g. Intra-Terminal Transportation (ITT)) and hinterland distribution can cause negative environmental impacts [1]. For example, ports need to reduce greenhouse gas emissions by avoiding traffic congestions or through the use of eco-friendly logistics vehicles. For this reasons, this growth must be supported by two sides: from the port surrounding areas point of view, by exploiting new and more efficient inland transport services/connections improving goods distribution with lower environmental impact; and from the port point of view, evolving the infrastructure using cutting-edge Information and Communication Technologies (ICT), which help to improve efficiency and the performance of the goods handling process.

Considering the port ICT infrastructure perspective, there are a number of different technologies that may improve the coordination of ITT operations. The availability and quality of information such as container locations, destinations, time windows, and available connections are essential to efficiently organize ITT operations [3]. Distributed Ledger Technology (DLT) has provided several implementations aiming to improve products tracking, from the producer to the consumer, and providing also the immutable tracing of seaport operations [4]. Exploiting cutting-edge communication technologies is the key to shorten the information sharing time, thus improving the whole ITT operations' delay. However, embracing digital transformation does not come without a price. Many seaport stakeholders, previously operating offline, will need to be connected to exchange information and to implement new digital processes, something that will inevitably lead to an increased attack surface, which can be exploited by malicious actors and compromise regular seaport operation. Just to give an example, in a fully connected ITT operations scenario an attacker can take remote control of logistic vehicles and cause accidents within the terminal area, possibly also involving quay operators. Additionally, an attacker may manipulate the database records with the wrong container destination or status information, thus causing a denial of supply-chain services and corresponding economical damage to terminal companies. In general, every attack that impairs the information *integrity* or the ITT services and operations *availability* leads to unpredictable consequences to the whole seaport operations management. For this reason, the adoption of a comprehensive security scheme is crucial to protect critical infrastructures such as seaports. Systems aiming to optimize and improve ITT operations must take into account their exposure to security issues and vulnerabilities and enforce mechanisms to neutralize them.

A. CONTRIBUTIONS OF THE PAPER

This paper proposes a fully customized security credential management system, able to track and authorize logistic vehicles, e.g. forklifts, within seaport container terminals during cargo and container movements. The proposed scheme takes advantage of a DLT-based Vehicular Public Key Infrastructure (VPKI) named IOTA-VPKI [5], customized for the logistics use case as described in Section IV-A. The customized version of IOTA-VPKI enables authentication and authorization operations compliant with EU and US Intelligent Transportation System (ITS) standards and supports logistic vehicles' misbehavior detection with the consequent certificate revocation to exclude malicious vehicles from the system. Additionally, the IOTA-VPKI implementation is extended to immutably store the forklifts and goods position in the underlying DLT, thus effectively tracking logistic vehicles and general cargo management events. The proposed scheme is designed to be compatible with any Terminal Operating System (TOS) to authorize logistic vehicles in the quay area. Finally, the COREALIS H2020 EU project framework is leveraged to test the effectiveness of the proposed security scheme, integrating the security credentials management system in the RTPORT module of the COREALIS architecture. Laboratory experiments demonstrate that the proposed security mechanism introduces negligible delay with respect to the total time of cargo movement. Furthermore, it is shown that the cargo release operation delay is not affected by the number of cargo movements, allowing us to conclude that it is fully compatible with container terminals of any size. A proof of concept prototype implementation was deployed in the Lorenzini's terminal in the port of Livorno, where the whole system was successfully tested in a real operational environment, thus demonstrating the effectiveness of the devised solution.

The rest of the paper is organized as follows: Section II presents the problem statement and briefly describes relevant background from vehicular and logistics point of view; Section III addresses relevant related work, whereas Section IV provides a detailed description of the proposed scheme, describes its components (i.e. IOTA-VPKI logistics customization and RTPORT) and extensively outlines the authentication scheme for logistic vehicles; in Section VI the experimental setup and test cases are presented together with the obtained results in both laboratory and real field environments; finally Section VII presents a discussion of the main findings of the paper and its conclusions.

II. BACKGROUND

A. INTELLIGENT TRANSPORTATION SYSTEMS

The most advanced sensing and communication technologies have been used in recent years to make vehicles more intelligent. The incorporation of Information and Communication Technologies (ICT) gave birth to a new generation of vehicles that will revolutionize transportation systems [5]. Furthermore, the emergence of Cooperative Intelligent Transportation Systems (C-ITS) and related technologies contributed to new services standardization, supporting new modes of transportation and traffic management, and allowing users to drive in a safer, more coordinated, and smarter way. New C-ITS-based services leverage the cooperation between road users and entities, which constantly broadcast awareness messages (e.g. traffic accidents, road conditions) used to evaluate the surrounding environment and take better informed and safer decisions. A typical C-ITS system is composed of two main entities: the first is installed in vehicles and is called the vehicle ITS station unit (V-ITS-SU), also commonly known as On-Board Unit (OBU), while the second is installed on the road and is called roadside ITS station unit (R-ITS-SU), also know as Road-Side Unit (RSU). The cooperation between road users described above is enabled by two types of communications, namely Vehicular-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications, which are established between vehicles and infrastructure entities. Generally speaking, thanks to C-ITS protocols and standards, vehicles can exchange safety messages exploiting V2V communications, and communicate directly with RSUs and other C-ITS infrastructure entities using V2I communications [6].

The cooperative ITS architecture, formally specified by ISO TC204 [11] and ETSI TC ITS [12], includes cross-layer vertical security ITS station entity, which provides standard security functionalities, responsible for performing the atomic security operations and for storing the credentials needed by the security protocols. The credentials used to secure C-ITS services are stored and maintained in the security entity. These include cryptography keys, authorization tickets, certificates, and other security-related parameters, which are usually stored in a Hardware Security Module (HSM). Currently, V2X security utilizes asymmetric cryptography signatures, both in ETSI ITS Security standards and in IEEE 1609.2. These standards essentially describe the security's architecture and management, trust and privacy models, threat vulnerability and risk analysis (TVRA), message and certificate formats, and Vehicular Public Key Infrastructure (VPKI) models [7].

The cornerstone component of the cooperative ITS architecture is the VPKI, which is entitled to enroll and authorize vehicles and road users in the system. Standardization bodies (i.e. Institute of Electrical and Electronics Engineers (IEEE) 1609.2 Work Group WG [8], [9], and European Telecommunication Standards Institute (ETSI) Technical Committee (TC) ITS WG 5 [10]) and harmonization effort (i.e. Car2Car Communication Consortium (C2C-CC) [13]) recognized VPKI as an effective security mechanism to assure the security of the C-ITS underlying communication infrastructure. The VPKI architecture encompasses a set of Trusted Authorities (TAs) which are responsible to manage different types of vehicles' credentials, namely Long Term Certificates (LTC - also known as Enrollment Credentials (ECs)) used to enroll vehicles in the system, and Short Term Certificates (STC - also known as Authorization Tickets (ATs)), which are used to authorize vehicles to access ITS specific services and assure the driver's anonymity in the system [7].

B. DISTRIBUTED LEDGER VEHICULAR PKI: IOTA-VPKI

The first version of IOTA-VPKI was presented in [5] as an adaptation of SECMACE credential management system [16]. SECMACE was proposed by *Khodaei et al.* and it is fully compliant with the current US and EU standards described and analyzed in Section II. The proposed Vehicular Public Key Infrastructure (VPKI) scheme takes the SECMACE reference architecture as the starting point and integrates it with an IOTA distributed ledger implementation as a storage backend of certificates issued to vehicles. As extensively described in [5], IOTA is a Distributed Ledger Technology (DLT) which leverages a Direct Acyclic Graph (DAG) ledger, well suited for devices with small resource capacity. From a vehicular perspective, each vehicle accesses the IOTA network by communicating with the nearest neighbor IOTA Reference Implementation (IRI) node.

The VPKI architecture is composed of a set of Trusted Authorities (TAs) with distinct roles: the Root Certificate Authority (RootCA) is the trust anchor of the whole system and authorizes both the Long Term Certificate Authority (LTCA) and the Short Term Certificate Authority (STCA) for issuing certificates to vehicles. The LTCA is responsible for vehicle enrollment in the system and LTC issuance; in turn, the STCA is responsible for vehicle authorization to access system applications by issuing STC. Finally, the Resolution Authority (RA) is responsible to resolve an STC to an LTC identity of the misbehaving, malfunctioning, or outdated vehicle.

To effectively integrate the credential management system with the IOTA DLT implementation, each TA in the IOTA-VPKI architecture is equipped with a local IRI node and an IOTA wallet to have direct access to the IOTA Tangle ledger. The IOTA wallet is protected by a *seed*, an 81 characters length string that acts like a private key to open the wallet. In this way the vehicles can access the IOTA network leveraging the trusted VPKI's IRI nodes, thus mitigating man-in-the-middle (MITM) attacks risk during vehicle-to-VPKI communications.

As detailed in [5], IOTA-VPKI uses IOTA *Masked Authenticated Message* (MAM) channels to manage and store certificates issued by LTCA and STCA, and to effectively implement communication channels between TAs and vehicles. These channels are used These channels use symmetric encryption and only the *channel owner* (i.e. TA) can publish new data to be delivered to the entities entitled to read it (i.e. vehicles) [19]. Using its wallet, each TA has its own MAM encrypted channel that is used for end-to-end secure communication with vehicles during certificate issuance/update procedure. IOTA-VPKI eliminates the single point of failure (SPoF) in TAs as they can be replicated transparently without vehicle reconfiguration. When a new instance of a specific STCA is created for replication, it uses the same *seed* of other available STCA instances to manage the same wallet and thus the same MAM channels. This avoids SPoF in TAs, known issue of TA-based VPKI [5], and increase the robustness against DDoS attacks as well as the availability level of the whole VPKI.

As discussed in [5], the main drawback of current MAM channel implementation stands behind the need to store messages in the IOTA *permanent* node to prevent deletion during *snapshot* processes [31]. This node requires large storage, bandwidth, and high speed, so it cannot be hosted on devices with small computational resources. The permanent node is called *Chronicle* and is a *permanode* solution which stores transactions in a distributed database that is secure and scales well [22]. Each IRI node instance running within the IOTA-VPKI TAs can be set up like a *Chronicle* node so that the

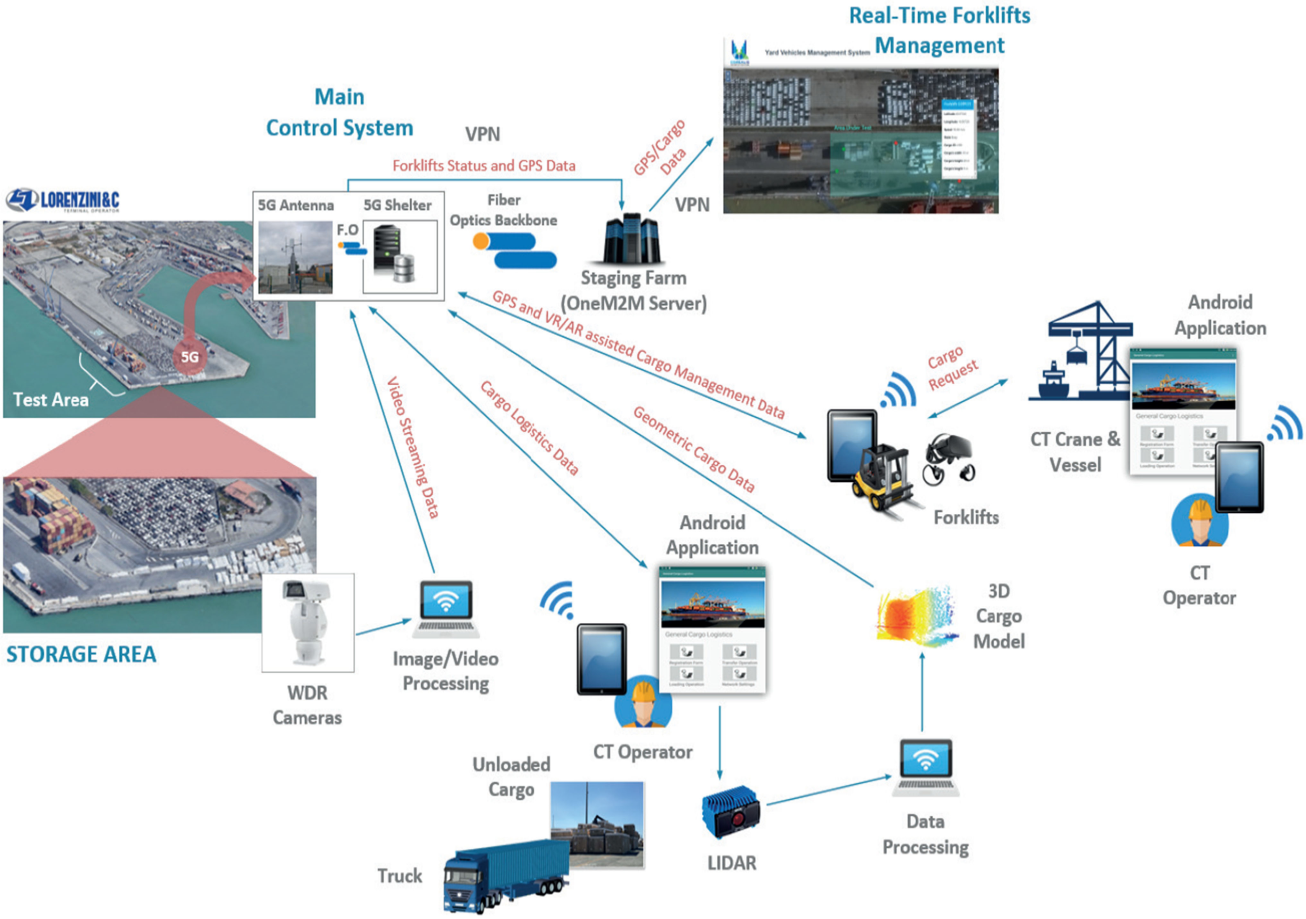


FIGURE 1. RTPORT module reference architecture.

zero-value transactions are permanently stored in the IOTA-VPKI for audit.

C. THE COREALIS PROJECT

The COREALIS EU project [15] proposes a strategic and innovative framework, based on pervasive and disruptive technologies (e.g. 5 G, IoT, Machine Learning, Virtual and Augmented Reality - VR/AR) to handle upcoming and future capacity, traffic, efficiency, and environmental challenges (e.g. inefficient usage of yard equipment and cargo management; high trucks' turnaround time; the impact of negative port decisions; and long vessels operation completion times). To this end, the project adopts a stakeholder-driven approach, considering the ports' and port-cities' main challenges to support the future shift to Industry 4.0. To address these challenges, COREALIS proposes a defined set of innovations implemented and tested in real operating conditions in 5 different Living Lab seaports (Piraeus, Valencia, Antwerp, HaminaKotka, and Livorno).

Employing these port-driven technological and societal innovations, the project allows to embrace of circular economy models in port strategy and operations. Using predictive models as well as advanced data analytics (i.e. *Marketplace* and *Predictor* system modules), it will be possible to minimize the meantime for trucks waiting at the port using an advanced *Truck Appointment System* (TAS), thus reducing the port's total environmental footprint associated with intermodal connections. The usage of 5 G connectivity in container terminals in the *Model-Driven Real-Time Control* (RTPORT) and *Process Modeling of Cargo and Data Flows* (PORTMOD) modules enables optimizing the yard capacity and the cargo handling automation. Finally, the *Port of Future Serious Game* (PoFSG) system module offers training and simulation tools that enable the ports' management board to take a better medium and long term strategic decisions.

D. RTPORT: MODEL-DRIVEN REAL-TIME CONTROL

The RTPORT is a standalone COREALIS system module designed to optimize the on-field general cargo management operations. The lack of automated systems in this field leaves quay operators alone during daily cargo loading/unloading operations, and operational mistakes happen quite often due to non-standard geometries of general cargo or routing faults. Fig. 1 depicts the RTPORT module architecture deployed in Lorenzini's terminal area within Livorno port. RTPORT consists of multiple interconnected smart IoT devices (i.e Wide

Dynamic Range (WDR) cameras and Laser Imaging Detection and Ranging (LIDAR) devices) managed by the Main Control System (MCS), which implements the core functionalities of the RTPORT module and communicates with other entities via 5 G network. The forklifts available in the terminal are managed by the *Real-Time Forklifts Management* (RTFM) component that feeds on-demand the MCS with the forklifts' status and position [23].

The data collected by the MCS from the IoT devices is analyzed to optimize the three main *phases* of the general cargo management process:

- *Registration:* unloading cargo from the truck that arrives to the terminal;
- *Storage:* storage cargo within the terminal dedicated general cargo area;
- *Loading:* loading cargo on the vessel.

When the truck arrives at the terminal and the cargo is unloaded, the quay operator uses a custom logistics application to update the cargo information (i.e. ID, destination and weight) and completes *Registration phase* within the MCS. Then the cargo is scanned by the LIDAR device to acquire its dimensions, so the 3D model of the cargo is stored in the MCS subsystem. At this point, the MCS will ask the *Real-Time Forklifts Management* (RTFM) for the nearest forklift *available* in the yard that will conduct the *Storage phase*, moving the cargo to the dedicated general cargo storage area. The forklift driver is then guided to the storage area utilizing AR/VR services running over a smart device installed on the forklift. Furthermore, the MCS applies an optimal cargo distribution algorithm based on the storage area layout and space to guarantee proper distribution of the cargo.

At this point, when new vessel berths at the terminal, the *Loading phase* will start: the quay operator on the crane asks the MCS for available cargo in the storage area that matches the information available in the loading plan provided by the vessel's captain. Once again, the MCS asks the RTFM for the nearest forklift *available* in the yard and performs the association between forklift and cargo. The driver is once again assisted by the forklift' AR/VR device to avoid unnecessary movements, thus minimizing loading delay. During this phase, WDR cameras allow the MCS to enable real-time cargo tracking, a fundamental step for the correct functioning of AR/VR-based services.

III. RELATED WORK

Several research endeavors describe security solutions for maritime port logistics. As a critical infrastructure (CI), maritime ports are extensively protected with Supervisory Control and Data Acquisition (SCADA) systems, that aim to control, monitor, and automate CI operations and processes. Due to the evolution of CI ICT infrastructures, SCADA systems are progressively integrating new technologies such as IoT, ITS, edge, and fog computing. Sajid *et al.* [25] described the security challenges of cloud-assisted IoT-based SCADA systems and provided a method to improve and maintain a high-security level of such systems. In [26], Baker *et al.* proposed identity-based cryptography and signature schemes to reinforce the integrity, security, and privacy of SCADA-based IoT CI at the fog layer. Also in [27] the open issues related to the security protection of IoT-enabled SCADA system were investigated. The authors emphasized physical, cyber, geographic, and logical CIs dependencies and interdependencies on other infrastructure (i.e. CI surroundings) to recognize the huge attack surface of the new generation of SCADA systems. One example of this kind of dependency is the integration of seaport CI with ITS to improve freight transportation or ITT operations in general. For example, a detailed description on how to develop and deploy a fully automated Truck Guidance System (TGS) was described in [28], considering the roles of port administration, technology providers, and stakeholders to exploit better the available resources and improve the capacity and efficiency of the seaport operations. The authors exploited Cooperative ITS technology to design automated TGS. Furthermore, they completed the investigation by interviewing logistics stakeholders from the ecosystem of the port of Antwerp, including the end-user point of view. As detailed in the rest of this paper, a similar approach is followed to build an effective security scheme that matches the requirements validated with final users. The compatibility between ITS technologies and logistics information systems has been further discussed in [29] and [30] aiming to provide an effective methodology to implement Vehicular Adhoc Network (VANET) technologies and standards in the multimodal logistics area.

The aforementioned research works provided no experimental results demonstrating the effectiveness of the proposed solutions in a real environment. Mainly, such research endeavors solely discussed the feasibility and methodology to integrate ITS technologies in the logistics workflow. Besides its fundamental role in seaport ITS integration, security needs to be further addressed and investigated, considering a comprehensive threat model that takes into account both logistic perspectives regarding vehicles and their operations.

IV. PROPOSED SCHEME

The integration of ITS technologies in the seaports environment represents a step forward towards efficient and digital seaports. The new security challenges introduced by such integration motivate the design of a new authentication scheme based on ITS technologies and customized for logistics vehicles, that augment Terminal Operating System (TOS) security capabilities and, consequently, the overall seaport security level. In the subsequent subsections, the Vehicular Public Key Infrastructure (VPKI) architecture, customized for logistics and based on our previous work IOTA-VPKI [5], is presented, together with the forklift authentication scheme with three different use cases covering all expected conditions that can be found in a real environment.

A. IOTA-VPKI LOGISTIC CUSTOMIZATION ARCHITECTURE.

The first version of IOTA-VPKI presented in [5] needs to be customized to effectively support logistic use case

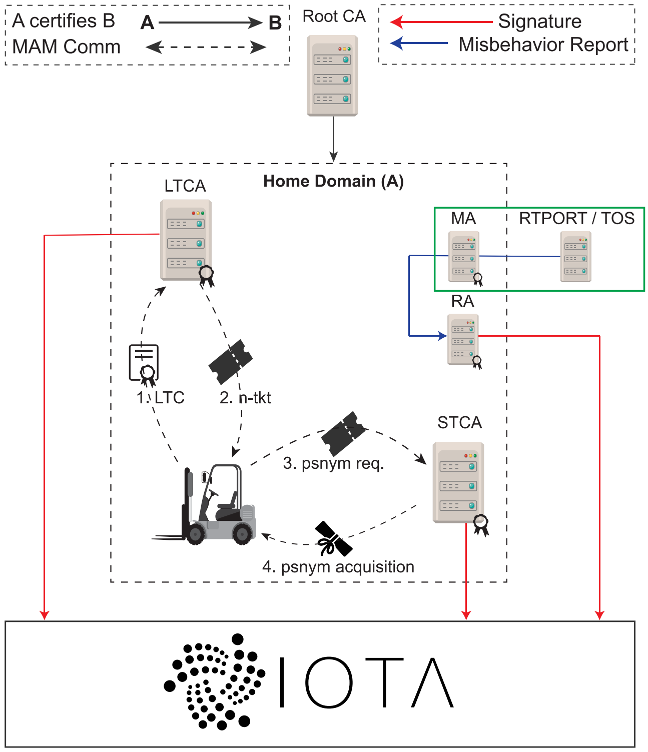


FIGURE 2. IOTA-VPKI Architecture: logistics customization.

requirements. In fact, the certificate revocation scheme supported by IOTA-VPKI leverages a *passive* revocation obtained *by expiry*. When a vehicle is recognized to be misbehaving and needs to be excluded from the system, the symmetric keys of the TAs' MAM channels are changed to effectively forbid further certificate requests from such misbehaving vehicle. This scheme can be seen as a Group Signature (GS) based approach, in which fully vehicle revocation is obtained by changing the shared symmetric key.

Unless this scheme is completely compatible with EU and US standards, it is not fully inline with security level of seaports. An *active* revocation mechanism needs to be employed to assure near real-time revocation of misbehaving logistic vehicles.

Thus, to support the logistic use case, we first assume that vehicles in seaports are equipped with an OBU (i.e. ITS station). In this way, the proposed scheme can be applied to other logistic vehicles, provided that they are equipped with a standard ITS station. When an OBU (δ) wants to send a message, it has first to acquire rights to access the C-ITS communications from the LTCA by sending its pre-registration recipe (step 1 and 2 in Fig. 2). Then, it negotiates rights to access the C-ITS services from STCA (step 3 and 4 in Fig. 2). Afterward, it digitally signs V2X messages with its private key K_s^δ (corresponding to the currently valid STC), and finally sends the message if and only if all the previous steps are successfully completed (namely the vehicle is considered *registered* and *trusted*).

Furthermore, a new version of IOTA-VPKI is designed to support logistic vehicle revocation and misbehavior detection. The revocation authority - RA functionalities are extended to implement an active certificate revocation method. The revocation *by expiry* passive scheme is substituted with a near real-time certificate revocation *active* method which leverages the underlying IOTA DLT: RA calculates the IOTA address corresponding to the hash representation of the certificate to be revoked and attaches a new *zero-value* transaction to the IOTA Tangle. The certificate revocation status verification corresponds to checking the *zero-value* transaction presence on the IOTA address corresponding to the certificate hash representation. The resulting transaction contains also the signature of the RA to avoid malicious actors revoking vehicles without authorization. Finally, the VPKI architecture is further extended to introduce a Misbehavior Authority (MA) that recognizes misbehaving logistic vehicles within the seaport area and notifies them to the RA for revocation.

B. FORKLIFT AUTHENTICATION SCHEME

The RTPORT architecture depicted in Fig. 1 does not include any security mechanism to enroll forklifts in the system. The complete absence of an authentication scheme exposes the whole COREALIS system to potentially dangerous attacks. For example, a malicious user can inject a false cargo position while the forklift driver is assisted by the AR/VR device, possibly causing an accident within the terminal area. Another attack could be performed against forklifts to communicate false *busy* status to RTFM, thus blocking the *Storage* and *Loading* phases described in the previous section.

To avoid these threats and minimize the attack surface of critical seaport infrastructures, we use the new version of the IOTA-VPKI described in Section IV-A to address the case of logistic vehicles in restricted areas. For this purpose, we first extended the forklift equipment with an OBU fully compatible with ETSI security standards. This scheme required a new version of the RTPORT architecture, capable of delegating the forklift enrollment, authorization, and revocation operations to the IOTA-VPKI platform. As a consequence, the RTPORT needed to be connected to the IOTA-VPKI, so the misbehavior authority could detect unauthorized behaviors of the logistics vehicles and, consequently, initiate the forklift's credential revocation process. The resulting architecture is able, not only to further secure the COREALIS system but can also be extended to other cases in which vehicles move in restricted private areas, e.g. airports, factories, military bases, etc.

Every forklift available in the terminal has to acquire a valid long-term certificate - LTC (step 1 and 2 in Fig. 2) to be listed as an *authenticated* forklift within the main control system - MCS. Then, whenever MCS selects a given forklift to move cargo (i.e. *cargoForkliftAssociation* function during *Storage* or *Loading* phases), it requests the forklift a valid short-term certificate - STC (step 3 and 4 in Fig. 2) to authorize the forklift to move the correct cargo. Finally, when the forklift arrives nearby the cargo, it needs to request the cargo release authorization to the MCS (i.e. *releaseCargo(cert(idCargo))*

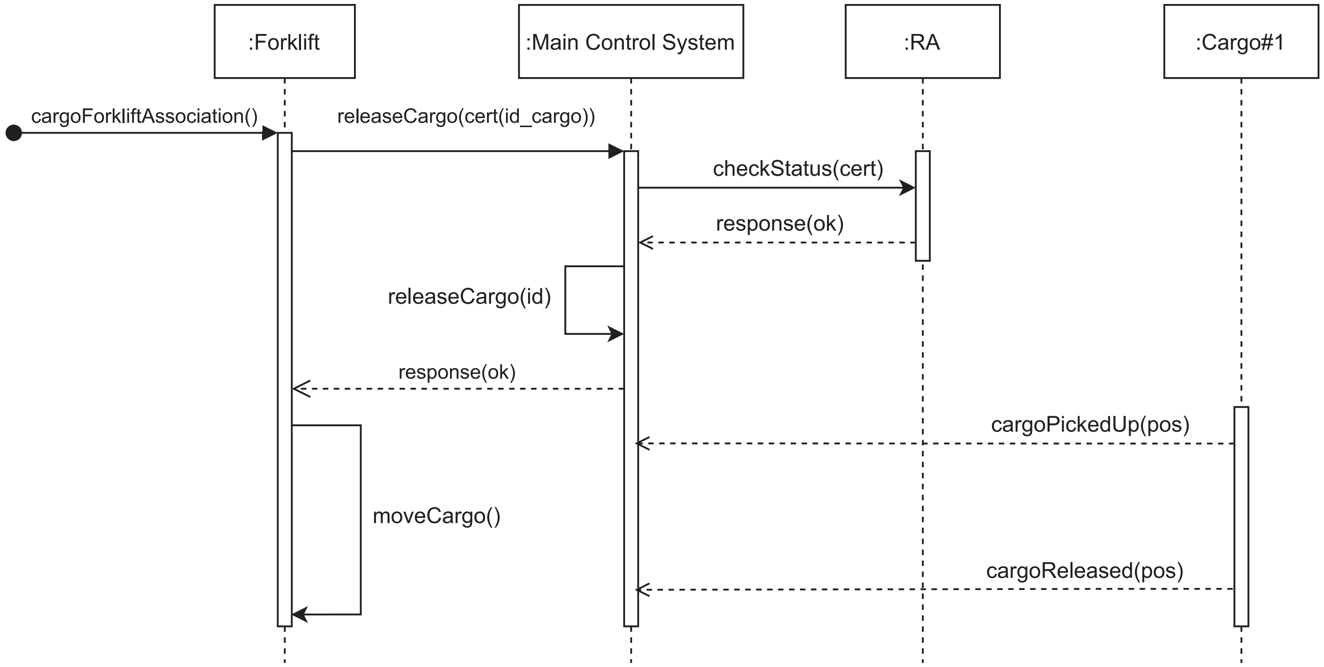


FIGURE 3. **Use Case 1 - Authorized Forklift takes cargo to a correct destination point.**

function in Fig. 3), by presenting the valid LTC containing the correct cargo ID: if the LTC is valid, the MCS enables real-time cargo tracking system and AR/VR device to assist the forklift driver; otherwise, a misbehavior reporting is done by MCS (i.e. RTPORT to MA communication depicted in Fig. 2) to IOTA-VPKI. At this point, the revocation authority - RA revokes valid certificates already issued to the misbehaving forklift, excluding it from the system by also revoking its long-term certificate - LTC, thus preventing new valid credential issuance to such forklift. The cargo is constantly monitored by the MCS during the handling operation thanks to the real-time cargo tracking and every unexpected movement can be detected and reported to the IOTA-VPKI for possible revocation. The real-time cargo tracking events are also stored on the IOTA distributed ledger to create an immutable and transparent cargo management event and forklift activity log storage. Thanks to the *feeless* scheme and the absence of miners, IOTA is specifically designed to be supported by devices with low computational capabilities, thus applicable also in the Internet of Things (IoT) scenario [17]. Furthermore, a public permissionless distributed ledger like IOTA could enable security information sharing between critical infrastructure worldwide, thus building a new concept of a global awareness system to respond to large-scale coordinated attacks.

Three different use cases, covering all the possible conditions expectable in a real environment, have been defined with the support of Lorenzini's terminal operators. The first use case, depicted in Fig. 3, represents a successful authorized movement of specific cargo from the dedicated general cargo storage area to the correct position under the crane. The real-time cargo tracking is represented with the *cargoPickedUp* and *cargoReleased* functions which model the cargo position change during handling operations. The second use case is depicted in Fig. 4 and shows the situation in which an *authenticated* forklift is *authorized* by the MCS to pick-up a given cargo, but the final release position of such cargo is not correct (i.e. cargo not released under the crane), leading to a misbehavior report (*notifyMisbehavior(cert)* in Fig. 4) made by the MCS to the IOTA-VPKI RA. Once the misbehavior is reported, the revocation authority revokes the forklift certificate, causing the forklift to be excluded from the system. The third use case is depicted in Fig. 5 and illustrates the *unauthorized* release request made by an *authenticated* forklift for the wrong cargo. In this case, when a forklift calls the *releaseCargo* function, the MCS checks if the forklift has been authorized to move the requested cargo and detects unauthorized access. At this point, the cargo is notified and alarms are activated in the general cargo area to alert terminal operators of misbehavior. Consequently, the MCS report forklift misbehavior to the IOTA-VPKI, causing the RA to revoke the forklift' certificate, thus enforcing the exclusion of the forklift from the system.

C. THREAT MODEL

The threat model considered in this work, takes into account the ETSI Threat, Vulnerability and Risk Analysis (TVRA) report for C-ITS, to identify possible threats and attacks that may affect the proposed scheme. The TVRA method is used to identify risks by isolating the vulnerabilities of the system, assessing the probability of malicious attacks on the recognized

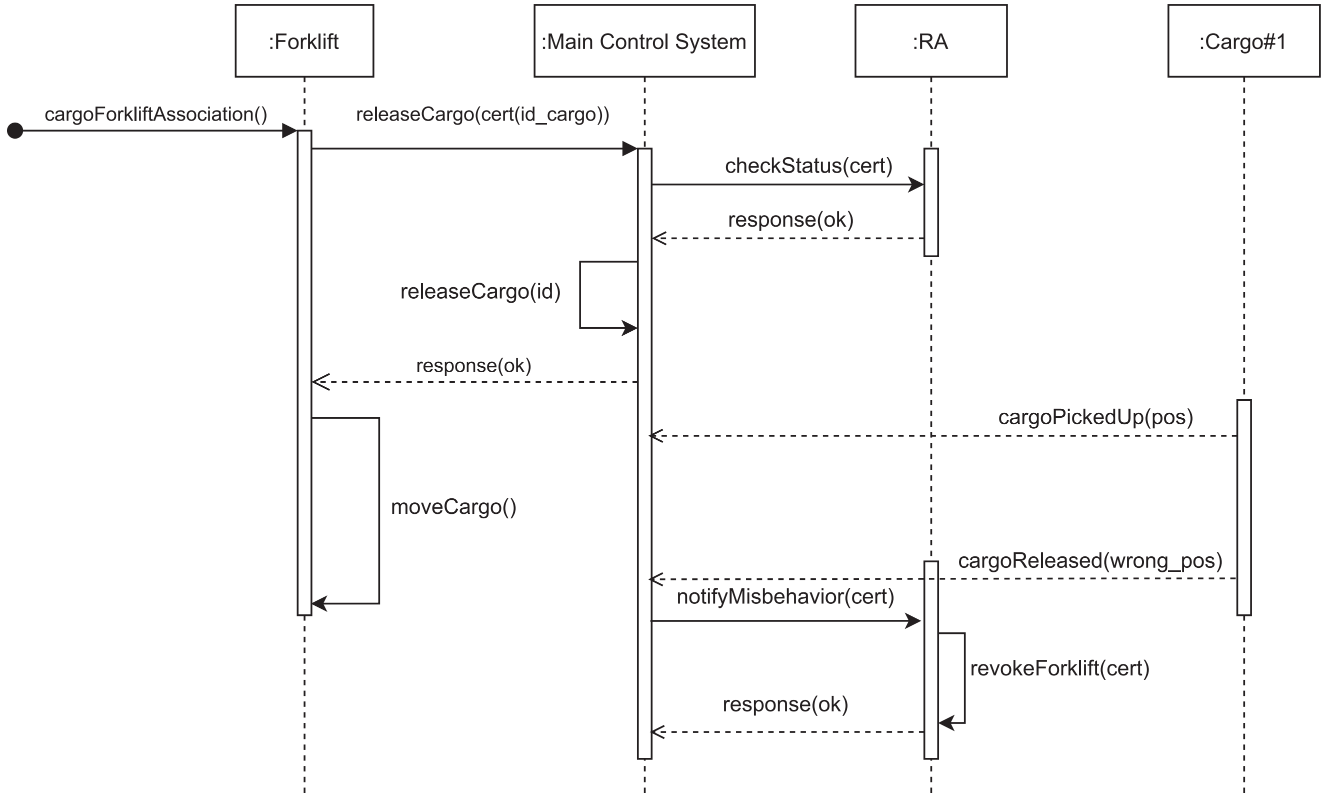


FIGURE 4. **Use Case 2 - Authorized forklift takes cargo to a wrong destination point.**

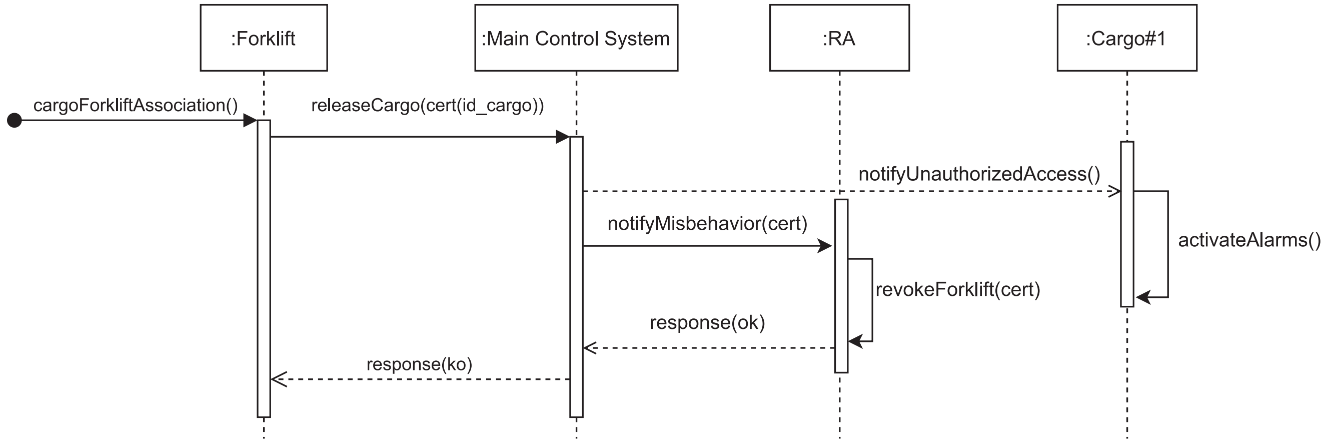


FIGURE 5. **Use Case 3 - Unauthorized Forklift is blocked while picking-up wrong cargo.**

vulnerability, and determining the impact when such attacks occur [24]. The generic security attributes for a C-ITS system are the following:

- *Confidentiality:* every information sent to or from an authorized entity should not be revealed to any party unauthorized to receive such information. Furthermore, it should not be possible for an unauthorized party to deduce the location, identity, and route taken by a vehicle based on its communication traffic information;
- *Integrity:* every information sent to or from an authorized entity should be protected from unauthorized modification, deletion, malicious modification, or manipulation during transmission;
- *Availability:* access to ITS services by authorized entities should not be prevented by malicious activity within the system;
- *Accountability:* it should be possible to audit all changes to security parameters and applications such as updates, additions, and deletions;
- *Authenticity:* it should not be possible for an unauthorized user to impersonate an authorized entity when communicating with other authorized parties.

These security attributes also apply to the logistics scenario considered in this paper. Hence, several threats considered for generic C-ITS systems must be examined in the scope of the proposed solution, namely:

- *Man-In-The-Middle attack:* a malicious actor can degrade the integrity of the proposed scheme by routing main control system - MCS certificate status requests to the attacker, thus impersonating Revocation Authority (RA). In this scenario the attacker induces the MCS to trust a revoked forklift, potentially causing dangerous consequences. The proposed scheme prevents this attack by inserting a RA signature within the certificate revocation status response, thus enabling the MCS to check the integrity and authenticity of the certificate revocation status information;
- *Denial of Service (DoS) attack:* considering the MCS as a Target of Evaluation (ToE), a malicious user can implement a message saturation attack to prevent forklift *releaseCargo* requests to arrive at the MCS: the proposed scheme mitigates such scenario without exposing the MCS on the public Internet and restricting access to the local network where the MCS and forklifts are connected, thus avoiding an unauthorized entity to reach MCS;
- *Manipulation of stored information attack:* malicious manipulation of stored certificate revocation status information may cause the MCS to trust a revoked forklift and permitting it to pick-up cargo that it is not entitled to move. The proposed scheme requires an asymmetric cryptographic signature applied by the IOTA-VPKI TAs and stored together with the revocation information to prevent manipulation: without the private keys it is not feasible for an attacker to manipulate or craft revocation information;
- *Insertion of information attack:* a malicious actor can insert crafted malicious information to degrade the integrity of the forklift's revocation information or status available in the system. In this scenario, once again, the MCS can be wrongly convinced to trust revoked forklifts and authorize them to move a specific cargo available in the terminal area. In this scenario, the IOTA-VPKI TAs' signatures (applied on each certificate and revocation information) assure the integrity and the authenticity of the credential management information to the MCS. In these conditions, it will be very difficult for an attacker to impersonate the IOTA-VPKI TAs and insert malicious information into the system.

Summarizing, the proposed authentication and authorization scheme is designed to protect a fleet of forklifts against *DoS*, *Manipulation of stored information*, *Insertion of malicious information*, and *Man-In-The-Middle* attacks. Furthermore, considering the security objectives and requirements stated in ETSI TVRA report [24], this scheme fulfills the *Availability*, *Integrity*, *Authenticity*, *Accountability* and *Confidentiality* requirements. Therefore, it represents a real demonstration that it is feasible to deploy secure C-ITS applications based on current standards.

V. OPERATIONS

In this section, we provide the details of the four fundamental operations of the proposed forklift authentication scheme: cargo-forklift association, release cargo, move cargo, and forklift misbehavior notification. However, for the sake of completeness, we start this section with a brief introduction to the primitive functions that are used by the operations.

A. PRIMITIVE FUNCTIONS

To implement the fundamental operations, the forklift authentication scheme uses different primitive functions to accomplish different tasks. We briefly introduce them to let the reader better understand the algorithms described in the following subsections.

Message functions: the message auxiliary functions are used to send a request/response message in the different algorithms described in the next sections. The following methods are used:

- $sendCertificateRequest(\rho)$: given a valid request ρ, the function performs a complete certificate request to the IOTA-VPKI;
- $replyToCertificateRequest(\mu)$: given a valid response message μ, the function sends the reply message to the entity that has requested a new valid certificate;
- $replyToReleaseCargoRequest(\mu)$: given a valid response message μ, the function sends the outcome of $releaseCargo$ operation (i.e. authorization granted or rejected) to the requesting entity;
- $replyToNotifyMisbehavior(\mu)$: given a valid response message μ, the function returns the revocation outcome to the Main Control System (MCS).

Cryptographic functions: the cryptographic functions are the ones related to the vehicular signcryption scheme used by the IOTA-VPKI. The following methods are used:

- $keygen^{sign}(\lambda)$: with a specific set of security parameters λ, the function called by an entity δ outputs an asymmetric key pair for signing (i.e. K_s^δ) and verification (i.e. K_v^δ) operations;
- $sign(K_s^\delta, m)$: given a specific K_s^δ issued to an entity δ, and a message m, the function outputs a signature σ over m;
- $verify(K_v^\delta, \sigma, m)$: given a specific K_v^δ issued to an entity δ, a message m, and the corresponding signature σ, the function verifies if the provided signature is valid for the message m.

IOTA Tangle functions: the IOTA Distributed Ledger Technology (DLT) specific functions are used to manage the transaction issuance, and they are the following:

- *tryte_encoder(m):* on input, an arbitrary string m, the function returns the IOTA address representation format of the provided string, namely an unique string of 81 trytes as described in [18];

- *attachToTangle(addr, m):* given a valid IOTA address *addr*, and an arbitrary message *m*, the function performs a zero-value transaction issuance and attaches it to the IOTA Tangle as described in [17].

IOTA-VPKI functions: the IOTA-VPKI functions are used by the RTPORT module to communicate with the VPKI. The considered functions are listed below:

- $authorizationValidation(Cert_\delta)$: on input a certificate $Cert_\delta$ issued by the IOTA-VPKI, the function returns the value *True* when the entity δ is entitled to receive the requested authorization level;
- $notifyMisbehavior(Cert_\delta)$: on input a certificate $Cert_\delta$ issued by the IOTA-VPKI, the function consumes the misbehavior report for the entity δ and eventually revokes it;
- $checkCertificateStatus(Cert_\delta)$: given a certificate $Cert_\delta$ issued by the IOTA-VPKI, the function verifies the validity of the provided certificate and returns the value *True* when $Cert_\delta$ is not revoked;
- $authorizeVehicle(vehicle\_id, cargo\_id)$: given a *vehicle_id*, and a cargo identifier (i.e. *cargo_id*), the function effectively authorizes the provided vehicle to move the specific cargo;
- $resolveIdentity(Cert_\delta)$: given a certificate $Cert_\delta$ issued by the IOTA-VPKI, the function resolves the real identity of the entity δ and returns its unique identifier.

Connected cargo functions: the connected cargo exposes different functions that are used to interact with the RTPORT module.

- *updateCargoState(s, cargo_id, p)*: given a new state *s*, for a given cargo identifier *cargo_id*, and a new position *p*, the function updates the current state of the cargo to the new one in the Real-Time Forklifts Management (RTFM) module. Possible values for *s* are: “blocked,” “pickedUp,” and “released”.
- *notifyUnauthorizedAccess(cargo_id)*: the function consumes a notification for unauthorized access to a specific *cargo_id*, and activate alarms to alert the surroundings of an unauthorized access;

Connected Forklift functions: the connected forklift exposes a single function that is used by MCS to communicate the cargo to be moved when a specific forklift is selected.

- $signal(F_i, cargo\_id, p)$: the function notifies the forklift F_i to move the selected cargo (i.e., *cargo_id*) to the destination position *p*.

B. CARGO-FORKLIFT ASSOCIATION

As described in Section II-D, the RTPORT module is equipped with the Real-Time Forklifts Management (RTFM) component that allows quay operators to see, in real-time, all the available forklifts within the general cargo terminal area. The RTFM module provides information on the status of each forklift (i.e. available or busy), the forklift-id, the forklift speed, and position within the quay area. Thus, the Main Control System (MCS) exploits this information to run a simple algorithm to select the best forklift that will be authorized to move a specific cargo under the crane. The cargo-forklift association method is reported in Algorithm 1.

Algorithm 1: Cargo-Forklift Association.

```
Input: $C$, $\{F_i\}_{i=1}^{N_F}$
  $Step$ 1 : select nearest forklift $F_n$ $with$ $1 \leq n \leq N_F$
  $C_{id} \Leftarrow id(C)$
  $C_{pos} \Leftarrow pos(C)$
  $F_{i_{pos}} \Leftarrow pos(F_i)$
  for all $F_i$ $in$ $\{F_i\}_{i=1}^{N_F}$ do
  if $F_i$ $is$ $available$ then
    $distances[i] \Leftarrow distance(C_{pos}, F_{i_{pos}})$
  else
    $distances[i] \Leftarrow \infty$
  end if
end for
  $F_{n_{id}} \leftarrow id(min(distances))$
  $Step$ 2 : authorize $F_{n_{id}}$ in IOTA-VPKI
  $signal(F_{n_{id}}, C_{id}, C_{pos})$
  $authorizeVehicle(F_{n_{id}}, C_{id})$
```

When the Main Control System (MCS) needs to select a forklift for a freight transfer, the logistic vehicle selection is done by the RTFM module in two steps.

Step 1: The cargo-forklift association algorithm is executed by the RTFM module. Two input parameters are considered for the set of forklifts in the area ($\{F_i\}_{i=1}^{N_F}$): status and position. The first refers to the forklift availability while the second reflects its position in the quay area. The cargo to be moved has a unique id (C_{id}) and it is also characterized its position in the quay area (C_{pos}). To guarantee the authenticity of the forklifts’ position, the RTFM module correlates the values received from the forklifts’ GPS with the output of the LIDAR devices available in the terminal increasing the precision of the measurements and, also, avoiding GPS spoofing.

The distance between the cargo (C) and each of the available forklifts ($\{F_i\}_{i=1}^{N_F}$) is computed and stored in a vector of $distances$. The id of the nearest forklift is then assigned to $F_{n_{id}}$.

Step 2: Finally, the MCS communicates the id of the cargo (C_{id}) and destination position (C_{pos}) to the selected forklift (i.e., $F_{n_{id}}$) via RTFM module, and notifies the IOTA-VPKI to accept authorization request to move the specific cargo under the crane.

As described in [2], the current RTPORT implementation uses a very simple algorithm to compute the geographical distance between the selected cargo (C) and the available forklifts. A possible extension of such algorithm can be implemented considering the shape of the general cargo terminal area. Shortest path algorithms can be considered to take into account obstacles between forklifts and the cargo to be moved. However, the specific shortest path algorithm that can be deployed in this scenario is out of scope of this work.

Algorithm 2: Short-Term Certificate Request.

```
Input: $C_{id},\ LTC_{F_{n_{id}}}$
  $(K_s^{F_{n_{id}}}, K_v^{F_{n_{id}}}) \Leftarrow keygen^{sign}(\lambda)$
  $m_{cr} \Leftarrow (K_v^{F_{n_{id}}} \mid LTC_{F_{n_{id}}} \mid C_{id})$
  $\sigma_{cr} \Leftarrow sign(K_s^{F_{n_{id}}},\ m_{cr})$
  $sendCertificateRequest(F_{n_{id}} \mid m_{cr} \mid \sigma_{cr})$
```

C. CERTIFICATE ISSUANCE

As described in the previous section, when the *Cargo-Forklift Association* operation ends, it notifies the selected forklift ($F_{n_{id}}$) to move the cargo C_{id} under the crane. To perform freight transport, the forklift needs to request the IOTA-VPKI to issue a new Short-Term Certificate (STC) as presented in Algorithm 2. To complete this operation, the forklift must have obtained a valid Long-Term certificate (LTC) from IOTA-VPKI with a procedure similar to the one described below.

The forklift ($F_{n_{id}}$) first generates a pair of asymmetric keys (i.e., a signing key $K_s^{F_{n_{id}}}$, and a verification key $K_v^{F_{n_{id}}}$) using the $keygen^{sign}(\lambda)$ cryptographic function, where the security parameters (λ) are the ones defined in IEEE 1609.2 standard [9] and are the same of the EU standards. The key generation described above is done every time a new (LTC or STC) certificate is requested: this guarantees fresh keys for each new certificate and lowers the risk to use compromised keys. Then, it prepares the certificate request (m_{cr}) message which contains the verification key ($K_v^{F_{n_{id}}}$), the valid LTC ($LTC_{F_{n_{id}}}$), and the cargo_id (C_{id}). Finally, the forklift digitally signs the message m_{cr} with its signing key ($K_s^{F_{n_{id}}}$) and sends the message coupled with the signature (σ_{cr}) to the IOTA-VPKI ($sendCertificateRequest$).

In turn, IOTA-VPKI executes the *Short-term Certificate Issuance* procedure to issue a valid STC as presented in Algorithm 3.

On receiving the message (m_{cr}), the IOTA-VPKI first checks the integrity of the message verifying the signature (σ_{cr}) with the received verification key ($K_v^{F_{n_{id}}}$). If the signature verification succeeds, the IOTA-VPKI checks that the requesting forklift ($F_{n_{id}}$) is the one selected by the MCS to move the provided cargo (C_{id}). Then, the IOTA-VPKI verifies that the provided $LTC_{F_{n_{id}}}$ is still valid (i.e., it has not been revoked), and requests the authorization request validation to the Long-Term Certification Authority (LTCA) using the $authorizationValidation$ function. If everything is correct, the IOTA-VPKI issues a new valid STC ($STC_{F_{n_{id}},C_{id}}$) and sends it to the requesting forklift ($F_{n_{id}}$) with a digitally signed certificate issuance (m_{ci}) response via the corresponding reply function ($replyToCertificateRequest$). Conversely, if the provided certificate ($LTC_{F_{n_{id}}}$) is not valid or the LTCA rejects the authorization request validation, the MCS digitally signs (σ_{ci}) a certificate issuance rejection message (m_{ko}), and sends it to the requesting forklift with the same reply function ($replyToCertificateRequest$).

Algorithm 3: Short-Term Certificate Issuance Procedure.

```
Input: $m_{cr},\ \sigma_{cr},\ m_{ok},\ m_{ko}$
Output: $STC_{F_{n_{id}},C_{id}}\ issued$
if $verify(K_v^{F_{n_{id}}}, \sigma_{cr}, m_{cr})$ then
  if $(F_{n_{id}}, C_{id})$ $was\ selected\ by\ MCS$ then
    if $checkCertificateStatus(LTC_{F_{n_{id}}})$ then
      if $authorizationValidation(LTC_{F_{n_{id}}})$ then
        $STC_{F_{n_{id}},C_{id}} \Leftarrow (STC_{F_{n_{id}}} \mid C_{id})$
        $\sigma_{ci} \Leftarrow sign(K_s^{VPKI}, STC_{F_{n_{id}},C_{id}})$
        $m_{ci} \Leftarrow (STC_{F_{n_{id}},C_{id}} \mid \sigma_{ci})$
      else
        $\sigma_{ci} \Leftarrow sign(K_s^{VPKI}\ m_{ko})$
        $m_{ci} \Leftarrow (m_{ko} \mid \sigma_{ci})$
      end if
     else
      $\sigma_{ci} \Leftarrow sign(K_s^{VPKI}\ m_{ko})$
      $m_{ci} \Leftarrow (m_{ko} \mid \sigma_{ci})$
    end if
    $replyToCertificateRequest(m_{ci})$
else
    $ignore\ message\ m_{cr}$
  end if
  else
  $ignore\ message\ m_{cr}$
  end if
```

D. CARGO TRACKING

The *cargo tracking* operation implements the real-time goods tracing in the proposed scheme. To this end, we defined three different cargo states as building blocks for cargo tracking plan:

- *locked:* this state models the moment when the cargo is fixed in the quay area. Each cargo move to this state just after the *storage* phase of the general cargo management process;
- *pickedUp:* a cargo move to this state whenever an authorized cargo picks it up from the field;
- *released:* this is the final state reached by the cargo whenever the forklift releases it under the crane during *loading* phase.

Once the forklift has loaded the unlocked cargo, the Main Control System (MCS) continuously receives position updates from the connected cargo and stores them in the underlying IOTA Tangle. In this way, the MCS is always aware of the current position of the cargo. Furthermore, it can recognize if the cargo is moving in the wrong quay zone and notify a forklift misbehavior.

E. RELEASE CARGO

The cargo needs to be unlocked by the MCS to be effectively moved under the crane. To this end, the selected forklift sends

Algorithm 4: Release Cargo.

```
Input: $STC_{F_{n_{id}},C_{id}}$, $K_v^{F_{n_{id}}}$, $\sigma_{rc}$, $m_{rc}$, $m_{ok}$, $m_{ko}$
  Output: $Authorization\ granted\ or\ rejected$
  if $verify(K_v^{F_{n_{id}}}, \sigma_{rc}, m_{rc})$ then
  if $checkCertificateStatus(STC_{F_{n_{id}},C_{id}})$ then
    $\sigma_{ack} \Leftarrow sign(K_s^{MCS}, m_{ok})$
    $replyToReleaseCargoRequest(m_{ok} \mid \sigma_{ack})$
    $await\ updateCargoState(``pickedUp," C_{id}, p1)$
    $await\ updateCargoState(``released," C_{id}, p2)$
    if $p2 \neq destination\_position$ then
      $\sigma_{nm} \Leftarrow sign(K_s^{MCS}, STC_{F_{n_{id}}})$
      $notifyMisbehavior(STC_{F_{n_{id}}} \mid \sigma_{nm})$
    end if
    else
    $\sigma_{nua} \Leftarrow sign(K_s^{MCS}, C_{id})$
    $notifyUnauthorizedAccess(C_{id} \mid \sigma_{nua})$
    $\sigma_{nm} \Leftarrow sign(K_s^{MCS}, STC_{F_{n_{id}}})$
    $notifyMisbehavior(STC_{F_{n_{id}}} \mid \sigma_{nm})$
    $\sigma_{ack} \Leftarrow sign(K_s^{MCS}, m_{ko})$
    $replyToReleaseCargoRequest(m_{ko} \mid \sigma_{ack})$
  end if
else
  $ignore\ message\ m_{rc}$
  end if
```

a *releaseCargo* request to the Main Control System (MCS). This operation is responsible to check that the requesting forklift is authorized to move the provided cargo_id. The details of *releaseCargo* method are presented in Algorithm 4. To effectively perform this request, the forklift asks to the IOTA-VPKI a new valid Short-Term Certificate ($STC_{F_{n_{id}},C_{id}}$) which explicitly authorizes the forklift $F_{n_{id}}$ to move the provided Cargo (C_{id}) as described in previous Section V-C.

The *releaseCargo* message (m_{rc}) sent by the forklift $F_{n_{id}}$ to MCS, is digitally signed using the asymmetric signing keys generated during the first step of the certificate issuance procedure. In fact, the verification of the provided signature (σ_{rc}) is the first action performed by the MCS upon receiving a new *releaseCargo* request. The signature verification step enforces the security attributes discussed in Section IV-C. If the verification succeeds, the MCS verifies the validity of the provided certificate ($STC_{F_{n_{id}},C_{id}}$), which in turn provides the id (C_{id}) of the Cargo to be moved under the crane. If the IOTA-VPKI confirms that the provided certificate is valid, the MCS unlocks the cargo and sends to the forklift $F_{n_{id}}$ the acknowledgment message (m_{ok}) with the corresponding digital signature (σ_{ack}) using the related reply function ($replyToReleaseCargoRequest$). Then, the MCS starts waiting for a cargo status update to the "pickedUp" new state with corresponding position ($p1$), and continuously monitors the moving cargo position waiting for the final cargo status update to the "released" state with the final position ($p2$). If this last position update is different from the destination_position, the MCS notifies the misbehaving forklift $F_{n_{id}}$ to the IOTA-VPKI which eventually revokes it.

Conversely, if the certificate is not valid, the MCS sends a notification to the connected cargo to activate alarms and to alert the surroundings about the unauthorized access ($notifyUnauthorizedAcess$). The input message contains the cargo_id (C_{id}) and the signature (σ_{nua}) applied by the MCS with its signing key (K_s^{MCS}). Finally, the MCS reports the forklift $F_{n_{id}}$ for misbehavior to the IOTA-VPKI with $notifyMisbehaviour$ function. Even in this case, the MCS digitally signs the input certificate ($STC_{F_{n_{id}}}$) and sends to the IOTA-VPKI the corresponding signature (σ_{nm}) coupled with the certificate of the misbehaving vehicle. In this case, the rejection message m_{ko} is digitally signed by the MCS (σ_{ack}) and sent to the requesting forklift with the corresponding reply function ($replyToReleaseCargoRequest$).

It is worth mentioning that we discussed the basic case when the cargo to be moved is directly accessible from the selected forklift. It is possible that the cargo is behind some other cargo that needs to be moved as well. In this particular case, the MCS authorizes the selected forklift to move the needed cargo at the time of *Cargo-Forklift Association* operation execution. In this way, the forklift asks the IOTA-VPKI for a *cumulative* STC which authorizes moving the different cargos.

F. FORKLIFT MISBEHAVIOR NOTIFICATION

When an unauthorized behavior is recognized by the MCS while the cargo is moving to the destination_position, a misbehavior alert is reported to the IOTA-VPKI to effectively revoke the misbehaving forklift and protect the system from malicious attacks. To this end, the *Forklift Misbehavior Notification* operation is executed by the MCS. As described in previous sections, the misbehavior notification can be issued in two different situations: when an authorized forklift moves a specific cargo to a wrong destination position; or when a forklift requests to move a cargo that is not entitled to transport to a specific destination. The *Forklift Misbehavior notification* operation is presented in Algorithm 5.

When the MCS recognizes a misbehavior it prepares a misbehavior report message m_{nm} containing the certificate ($STC_{F_n,C_{id}}$) of the misbehaving forklift F_n. To assure authenticity and integrity of the message, the MCS sends also the signature (σ_{nm}) of the message m_{nm} performed with the MCS's signing keys created during the certificate issuance procedure. In turn, upon receiving a misbehavior notification, the IOTA-VPKI first verifies the signature of the message with the provided verification key (K_v^{MCS}), and then resolves the real identity of the misbehaving forklift using the provided certificate $STC_{F_n,C_{id}}$. The forklift identity corresponds to a specific identifier (F_n) that the IOTA-VPKI uses to check the number of misbehavior reports ($reports(F_n)$) already received for the specific forklift. If this number is greater than the predefined threshold, the forklift (F_n) is removed from the authorized forklifts list and revoked from the system. Otherwise, the number of misbehavior reports is

Algorithm 5: Misbehavior Notification.

```
Input: $STC_{F_{n_{id}},C_{id}}$, $K_v^{MCS}$, $m_{nm}$, $\sigma_{nm}$, $m_{ok}$, $m_{ko}$, $m_{nop}$
Output: $Forklift\ successfully\ revoked$
  if $verify(K_v^{MCS}, \sigma_{nm}, m_{nm})$ then
  $F_n \Leftarrow resolveIdentity(STC_{F_{n_{id}},C_{id}})$
  if $reports(F_n) > threshold$ then
    $authorized\_forklifts.remove(F_n)$
    $iota\_address \Leftarrow tryte\_encoder(STC_{F_n,C_{id}})$
    $\sigma_{ri} \Leftarrow sign(K_s^{RA}, STC_{F_n,C_{id}})$
    $m_{ri} \Leftarrow (STC_{F_n,C_{id}} \mid \sigma_{ri})$
    $transaction \Leftarrow attachToTangle(iota\_address, m_{ri})$
    if $transaction\ is\ attached$ then
      $\sigma_{mr} \Leftarrow sign(K_s^{RA}, m_{ok})$
      $m_{mr} \Leftarrow (m_{ok} \mid \sigma_{mr})$
    else
      $\sigma_{mr} \Leftarrow sign(K_s^{RA}, m_{ko})$
      $m_{mr} \Leftarrow (m_{ko} \mid \sigma_{mr})$
    end if
  else
    $reports(F_n) \Leftarrow reports(F_n) + 1$
    $\sigma_{mr} \Leftarrow sign(K_s^{RA}, m_{nop})$
    $m_{mr} \Leftarrow (m_{nop} \mid \sigma_{mr})$
  end if
  $replyToNotifyMisbehavior(m_{mr})$
else
  $ignore\ message\ m_{nm}$
end if
```

simply incremented by a unit. The outcome of this revocation is twofold: on the one hand, the misbehaving forklift is removed from the authorized forklift list in the RTFM (i.e. $authorized\_forklifts.remove(F_n)$); on the other hand, the provided $STC_{F_n,C_{id}}$ is revoked by the IOTA-VPKI, publishing a transaction on the IOTA DLT at the address ($iota\_address$) representing the unique *tryte_encoded* representation of STC. The IOTA transaction message (m_{ri}) is created concatenating the certificate ($STC_{F_n,C_{id}}$) and the corresponding digital signature (σ_{ri}) to enforce the integrity of revocation information. In this way, the misbehaving forklift will be not allowed to move other cargos, and any new authorization request by F_n (i.e. F_n) will be refused by the IOTA-VPKI. If the transaction is successfully attached to IOTA DLT, a success message (m_{ok}) is digitally signed by the IOTA-VPKI (σ_{mr}) and correctly saved in the corresponding variables. Conversely, when the misbehavior threshold is not exceeded, the response message (m_{mr}) is updated with the no-operation message m_{nop}, and then digitally signed (σ_{mr}) by the IOTA-VPKI.

Once the algorithm is finished, the misbehavior response message (m_{mr}) is sent back to the requesting vehicle with the corresponding reply function ($replyToNotifyMisbehavior$).

The predefined threshold can be configured by the quay and terminal operators during the forklift registration phase and can be managed based on real conditions via the MCS and the RTFM. The threshold effectively represents the sensibility of the whole system to malicious attacks targeting the automated freight transport.

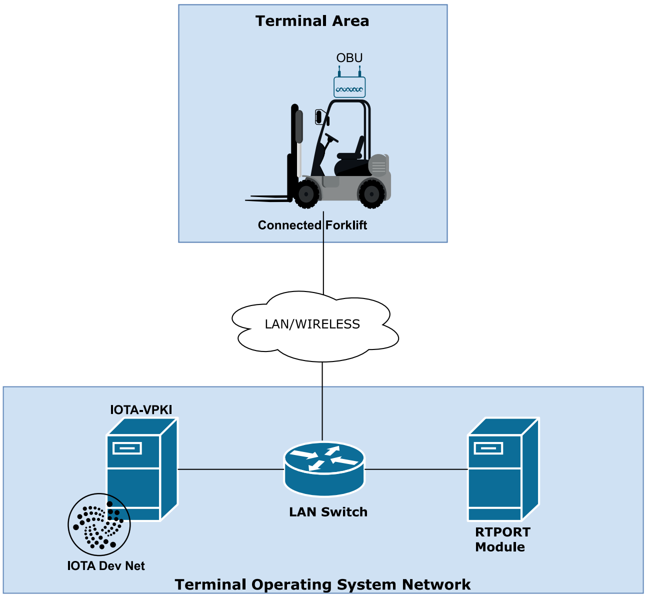


FIGURE 6. Experimental environment architecture.

VI. PERFORMANCE EVALUATION

To demonstrate the effectiveness of the proposed solution, two sets of experiments were conducted. The first experiments were done in a pseudo-real environment, deployed in the laboratory, while the second was performed in a field trial session at Lorenzini's terminal, within the Livorno port to evaluate the effectiveness of the proposed solution in a real environment. The following subsections describe the experimental settings for the two sessions and discuss the final results.

A. EXPERIMENTAL SETTINGS

The goal of the laboratory experiments is to demonstrate that the proposed security scheme applies to any terminal class size and that it has a negligible delay with respect to the end-to-end duration of a cargo movement. For this reason, a testing environment, closely mimicking a real scenario, was designed to evaluate the latency introduced by the proposed security scheme and assess its performance. The experimental environment architecture is depicted in Fig. 6. On the simulated Terminal Operating System (TOS) network, two identical workstations with 3.0-GHz Intel Core i5 CPU and 8-GB RAM were used to deploy an instance of the RTPORT module equipped with the security extensions described in Section IV, and an instance of the IOTA-VPKI extended with the proposed forklift revocation scheme. The workstations were interconnected through a 1-Gb/s Ethernet switch. In turn, on the quay area, a connected forklift is simulated with an ITS station (OBU), equipped with a SOM NXP i.MX 8 M Quad-core (4 x Cortex-A53 1.5 GHz) and 4 GB of RAM. The connected forklift simulates the release cargo procedure in different runs. All delay measurements were taken in the OBU to avoid potential timing synchronization issues.

The experimental setup for the field test sessions was identical to the one adopted in laboratory experiments, except for the 4 G wireless connection between the connected forklift and RTPORT Module, instead of the Ethernet network.

Due to the impossibility of blocking the daily terminal operations to execute multiple test sessions in the real environment, only twenty runs of each use case were executed over two days at the Lorenzini's general cargo dedicated area. However, all runs were successfully completed without issues and the obtained results were very similar to those obtained in the laboratory.

To avoid interference with public transactions, a private IOTA Tangle was employed in the IOTA-VPKI instance [20]. The private Tangle instance was executed with basic settings equal to Devnet [21]. Notice that the proposed method is *technically* compatible with the public IOTA Tangle instance. However, to better explain the *timing* compatibility between public and private IOTA instances, it is worth discussing the concept of *approved* transactions. The full process of attaching a transaction to the Tangle is detailed in [31]. At the end of such process, the new transaction is called a *tip*, i.e. an unapproved transaction. Each new *tip* waits for a confirmation through direct or indirect approval until its accumulated weight reaches the predefined threshold [31] at which point the *tip* becomes an *approved* transaction. The delay of this *approval* process depends on the number of network users and the predefined weight threshold. Furthermore, this delay impacts the number of confirmed transactions per second and it is the main difference between the IOTA Mainnet, i.e. public IOTA Tangle, and other kinds of IOTA networks, including private ones. However, our scheme does not depend on the *approval* process because vehicles can trust the content of new transactions even when they are in the *tip* state thanks to the Trusted Authority (TA) cryptographic signature, which is applied on every content published in the ledger. For this reason, we expect to experience comparable delays even using the public available IOTA Tangle.

B. EXPERIMENTAL RESULTS

The main goal of the proposed scheme is to provide a security layer that can authenticate, authorize, and eventually revoke forklifts in the RTPORT module. Hence the most important fact to be analyzed is the *vulnerability window*, i.e., the period in which a recognized misbehaving forklift remains trusted by the Main Control System (MCS) and other entities, potentially exposing the quay operators and the cargo to damage and accidents. For this reason, time measurements were focused on the *releaseCargo* function, since it is the MCS's operation that recognizes potential misbehaving forklifts. Since the *releaseCargo* function delay also includes the time to receive a Short-Term Certificate (STC) from the IOTA-VPKI, this certificate issuance delay was also measured at the connected forklift side to measure the impact of VPKI operations' on *releaseCargo* delay.

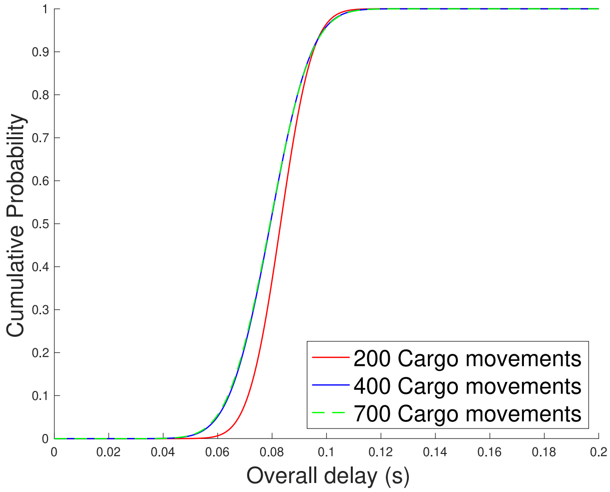


FIGURE 7. CDF of release cargo operation delay.

TABLE 1. Release Cargo Operation Delay Statistics

# Cargos	Minimum	Average	Maximum	$\Pr\{t \leq x\} = 0.95$
200	50 ms	83 ms	98 ms	98 ms
400	40 ms	80 ms	104 ms	99 ms
700	33 ms	80 ms	108 ms	99 ms

To set up the first experimental testing campaign in the laboratory, Lorenzini's terminal managers were interviewed to help to define the profiles of the different test runs in terms of the number of cargo available in the quay area. It was concluded that the volume of non-containerized cargo (i.e. general cargo) moved in a day depends on the size of each vessel and on the number of berths that are available in the terminal. Based on this information, three different general cargo terminal sizes were defined:

- *Small* size general cargo terminals move no more than 200 volumes per day;
- *Medium* size general cargo terminals move no more than 400 volumes per day;
- *Big* size general cargo terminals move no more than 700 volumes per day.

Thus, to demonstrate that the proposed method is independent of the volume of cargo moved, three different test runs were set up in the laboratory, each of them simulating one of the general cargo terminal class sizes defined.

Fig. 7 presents the Cumulative Distribution Function (CDF) of the release cargo operation delay in the three different general cargo terminal size profiles. The release cargo operation delay encompasses the STC issuance and the *releaseCargo* function call delays. As summarized in Table 1, in the first run (200 cargo movements) there is a 95% of probability that the delays are lower or equal to 98 ms. Increasing the number of cargo movements has almost no impact on the delay for the 95% probability since for 400 cargo movements the delay is 99 ms and the same delay is measured for 700 cargo movements. The average delay value is close to 80 ms in all

TABLE 2. Certificate Status Checking Delay Statistics

# Cargos	Minimum	Average	Maximum	$\Pr\{t \leq x\} = 0.95$
200	3 ms	11 ms	17 ms	15 ms
400	3 ms	10 ms	18 ms	15 ms
700	3 ms	11 ms	35 ms	15 ms

TABLE 3. STC Issuance Delay Statistics

# Cargos	Minimum	Average	Maximum	$\Pr\{t \leq x\} = 0.95$
200	16 ms	39 ms	51 ms	51 ms
400	17 ms	38 ms	53 ms	52 ms
700	16 ms	38 ms	53 ms	52 ms

three runs, while the minimum delay values are very different (50 ms in the first run; 40 ms in the second run; and 33 ms in the third run). On the contrary, the maximum values are close to 99 ms for all three runs. The results' trend shows that the delay of the proposed scheme is fully independent of the number of cargo movements. The constant delay in different runs suggests that the proposed solution can be applied in seaports of any class size.

However, it is worth noting that all runs correspond to authorized and successful cargo movements. Thus, the only operation done by the MCS is to verify the certificate forklift revocation status (lines 1–9 in Algorithm 4). As detailed in Section IV, the certificate revocation status checking consists of probing the IOTA address representing the forklift's certificate for a zero value transaction. The related delay statistics are presented in Table 2. Similarly to release cargo operation delay statistics, the revocation checking delay is almost equal and constant in the three different runs. In fact, in all runs, there is a 95% of probability that the delays are lower or equal to 15 ms. Regarding average values, the first and third runs measure 11 ms, while in the second run the average delay is 10 ms. In the worst-case analysis, the maximum value is measured in the third run (35 ms), while in the first and second runs the maximum value is close to 18 ms. Finally, the minimum values are equal to 3 ms in the three different runs. This constant trend justifies the approximately constant delay measured by release cargo operation. The remaining part of the Algorithm 4 is related to misbehavior notification (lines 11-13). The related delay is not experienced by the system in terms of vulnerability window because the first action of MCS is to remove the misbehaving forklift from the list of authorized vehicles (line 4 of Algorithm 5). This design assures approximately real-time revocation for each misbehaving logistic vehicle that has passed the pre-defined misbehavior threshold configured in MCS. In turn, this effectively demonstrates that the proposed scheme assures a very low vulnerability window regardless of the volume of cargo moved.

The laboratory results were further analyzed to assess the STC issuance delay statistics and see how the IOTA-VPKI forklift authorization operation impacts the delay of the proposed scheme. As summarized in Table 3, in the first run with 200 cargo movements there is a 95% of probability that the STC issuance delay is lower or equal than 51 ms, while in the second and third runs the same probability value applies for delays lower or equal than 52 ms. The average values are close to 40 ms in all three runs and, similarly, the minimum values are also very close: 16 ms for first and third runs and 17 ms for the second one. Finally, the maximum values are close to 50 ms in all three runs. Once again the constant trend of these results is motivated by the issuance process defined by the US and EU standards, which is exploited by the IOTA-VPKI. Because the issuance process relies on cryptographic operations whose complexity does not change, an approximately constant delay is to be expected when such operations are executed on a fixed hardware/software setup.

Considering the laboratory results, we can conclude that the highest contribution of release cargo operation delay presented in Table 1 is given by STC issuance procedure defined by US and EU standard. Our proposed scheme goes beyond the industrial state of the art and introduces new fundamental functionalities with a negligible delay with respect to the current standards.

Finally, to demonstrate that the proposed scheme works in a real environment, an instance of the RTPORT secured with the forklift authentication scheme described in Section IV-B was deployed in the Lorenzini's terminal, within the general cargo dedicated area in Livorno port (Italy). With almost 400 maximum daily cargo movements, Lorenzini's terminal is considered a *medium* class size general cargo terminal. A satellite photo of Lorenzini's terminal is presented in Fig. 8. To mimic the same conditions of the laboratory testing campaign, two forklifts were equipped with OBUs (i.e. red trapezoid in the center of the Fig. 8) and a publicly accessible instance of IOTA-VPKI, equipped with IOTA Private Tangle, was deployed. As discussed in Section VI-A, the ITS Station (OBU) employed in the field trial has been configured with the same characteristics used in laboratory experiments (i.e. SOM NXP i.MX 8 M Quad-core (4 x Cortex-A53 1.5 GHz), 4 GB RAM). Similarly, the workstations used to deploy the IOTA-VPKI instance, and the secured RTPORT module were identical to the one used in laboratory experiments. The only different setting is related to the 4 G wireless connectivity between OBU and Terminal Operating System (TOS) network as depicted in Fig. 6.

Twenty runs of the three use cases described in Section IV-B were performed, with the support of Lorenzini's terminal operators that drove the forklifts during use case runs. A single run represents a full cargo movement from the general cargo storage area (i.e. green trapezoid, top-right corner in Fig. 8) to the crane of the selected vessel (i.e. blue rectangle, bottom-left corner in Fig. 8). During the execution of tests, the *releaseCargo* function call and the STC issuance delay were measured from the OBU and their values are comparable with the ones measured in the laboratory environment. Considering the worst-case analysis, the maximum value measured during the field trial tests was 759 ms: comparing this value with the 95^{th} percentile (99 ms) reported in Table 1 suggests that the

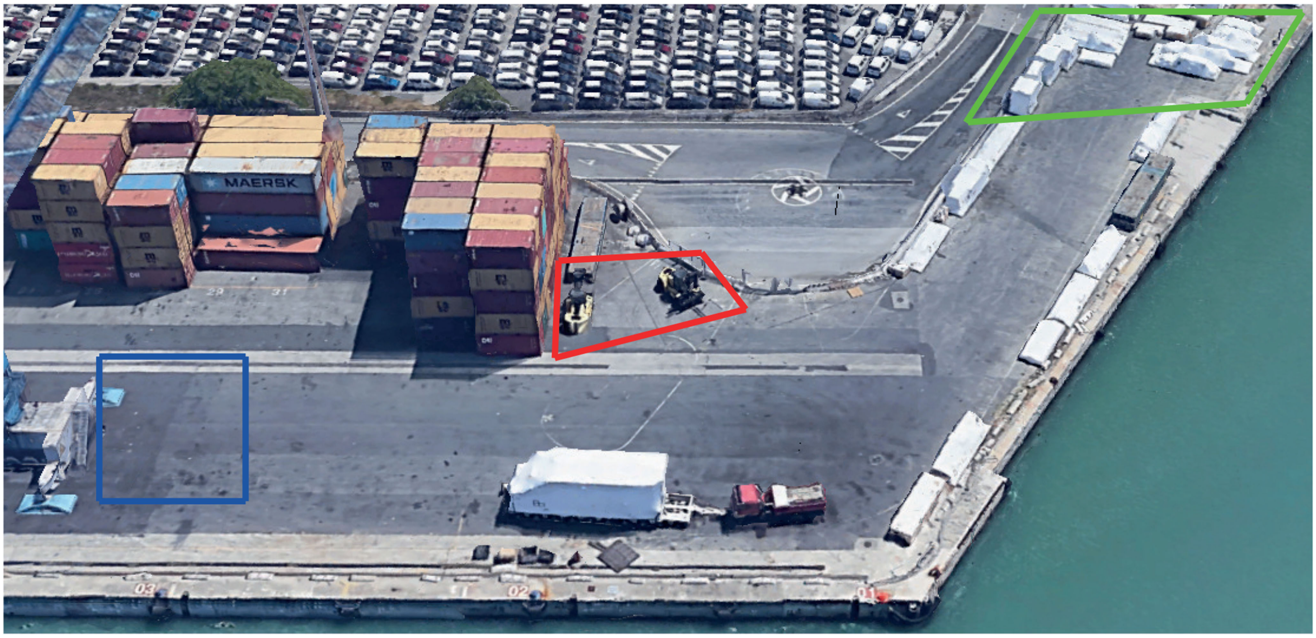


FIGURE 8. Lorenzini's terminal general-cargo area.

proposed scheme is performing as expected also in a real environment and that even in the worst-case scenario it introduces negligible delay with respect to the total cargo movement time (around 20–30 seconds in the Lorenzini's terminal).

VII. CONCLUSION

This paper presented a credential management system to authenticate and authorize logistic vehicles in seaport environments. The authorization process is essential to entitle a specific connected logistic vehicle to pick-up the correct cargo within the terminal area. The proposed solution is based on IOTA-VPKI [5], a Distributed Ledger based vehicular public key infrastructure compliant with US and EU standards. The IOTA-VPKI was customized to track seaport logistic vehicles and general cargo, exploiting the underlying distributed ledger technology as transparent storage of such tracking information. Furthermore, the proposed solution adopts a threat model based on the ETSI TVRA report [24] to address the security requirements and the robustness of the system against different types of attacks.

Different seaports class sizes has been considered, in terms of the number of cargo movements, to test the effectiveness of the proposed solution. Experimental results have shown that 95% of the release cargo operation (i.e. general cargo pick-up) delay are lower or equal to 99 ms, thus demonstrating the feasibility of the proposed scheme, which is completely independent of seaport class size (i.e. number of daily cargo movements). Furthermore, the H2020 COREALIS project testbed available in Lorenzini's terminal in Livorno port has been leveraged to test the proposed solution in a real environment. The field trial results demonstrate that the maximum delay was 795 ms, a value compatible with laboratory measurements and further prove that the proposed scheme performs as expected also in real conditions. Finally, the delay introduced in the proposed solution is negligible with respect to the total cargo movement time, which is, on average, greater than 20 seconds.

To summarize, the proposed solution can be used in any class size seaports to authenticate, authorize, and eventually revoke logistic vehicles within terminal areas. The proposed scheme mitigates the risks of intra-terminal accidents and enhances the security level of the whole seaport.

ACKNOWLEDGMENT

The authors would like to thank *Lorenzini & C.* terminal operator (https://lorenziniterminal.it/) and its employees for providing support in the use case definition and testing in the quay area.

REFERENCES

[1] "COREALIS Deliverable 3.1: Intra-terminal operations state of the art review," Accessed: Apr. 2, 2021. [Online]. Available: https://www.corealis.eu/wp-content/uploads/2020/02/D.3.1-Intra-Terminal-Operations-State-of-the-Art-Review.pdf

[2] "COREALIS Deliverable 5.4: Livorno Living Lab (LL) scoping document." Accessed: Apr. 2, 2021. [Online]. Available: https://www.corealis.eu/index.php/material-hub/

[3] L. Heilig and S. Voß, "Inter-terminal transportation: An annotated bibliography and research agenda," *Flexible Serv. Manuf. J.*, vol. 29, no. 1, pp. 35–63, 2017.

[4] E. Vieira, J. Ferreira, and P. C. Bartolomeu. "Blockchain technologies for IoT applications: Use-cases and limitations," *Proc. 25th IEEE Int. Conf. Emerg. Technol. Factory Automat*, vol. 1, 2020, pp. 1560–1567.

[5] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto, and P. Pagano, "IOTA-VPKI: A DLT-based and resource efficient vehicular public key infrastructure," *Proc. IEEE 88th Veh. Technol. Conf.*, Chicago, IL, USA, 2018, pp. 1–6.

[6] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[7] B. Fernandes, "Implementation and analysis of IEEE and ETSI security standards for vehicular communications," *Mobile Netw. Appl.*, vol. 23, pp. 469–478, 2018.

[8] *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*, IEEE Standard 1609.0, 2019.

[9] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Security Services for Applications and Management Messages - Amendment 2: PDU Functional Types and Encryption Key Management*, IEEE Standard 1609.2, 2019.

[10] "Intelligent transport systems (ITS); Security; ITS communications security architecture and security management," Eur. Telecommun. Standards Inst (ETSI)., Tech. Specification 102940, version 1.3.1, 2018.

[11] *Intelligent Transport Systems — Communications Access for Land Mobiles (CALM) — Architecture*, ISO Standard 21217, Int. Org. Standardization, 2014.

[12] *Intelligent Transport Systems (ITS); Communications Architecture*, Eur. Telecommun. Standards Inst. (ETSI) European Norm 302 665, version 1.1.1, 2010.

[13] "CAR 2 car communication consortium official website," Accessed: Apr. 2, 2021. [Online]. Available: https://www.car-2-car.org/

[14] "C-ROADS - the platform of harmonised C-ITS deployment in Europe," Accessed: Apr. 2, 2021. [Online]. Available: https://www.c-roads.eu/platform.html

[15] "COREALIS H2020 project website," Accessed: Apr. 2, 2021. [Online]. Available: https://www.corealis.eu/

[16] M. Khodaei, H. Jin, and P. Papadimitratos, "SECMACE: Scalable and robust identity and credential management infrastructure in vehicular communication systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1430–1444, May 2018.

[17] "IOTA transactions documentation," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/getting-started/0.1/transactions/transactions

[18] "IOTA addresses documentation," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/getting-started/0.1/clients/addresses

[19] "IOTA masked authenticated messaging documentation," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/client-libraries/0.1/mam/introduction/overview

[20] "IOTA: Set up a private tangle," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/compass/0.1/how-to-guides/set-up-a-private-tangle

[21] "IOTA networks," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/getting-started/0.1/network/iota-networks

[22] "IOTA chronicle documentation," Accessed: Apr. 2, 2021. [Online]. Available: https://docs.iota.org/docs/chronicle/1.1/overview

[23] "RTPORT: The 5G-based model-driven real time module for general cargo management," Accessed: Apr. 2, 2021. [Online]. Available: https://www.corealis.eu/wp-content/uploads/2020/03/IPIC2019_Full_Paper_CNIT_ERICSSON_v1.0_20_06_2019_updated.pdf

[24] "Intelligent transport systems (ITS); security; threat, vulnerability and risk analysis (TVRA)," Eur. Telecommun. Standards Inst. (ETSI), Tech. Rep. 102 893, version 1.2.1, 2017.

[25] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[26] T. Baker *et al.*, "A secure fog-based platform for SCADA-based IoT critical infrastructure," *Software: Pract. Experience*, vol. 50, no. 5, pp. 503–518, 2020.

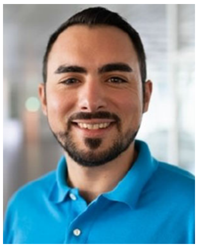
[27] N. Tariq, M. Asim, and F. A. Khan, "Securing SCADA-based critical infrastructures: Challenges and open issues," *Procedia Comput. Sci.*, vol. 155, pp. 612–617, 2019.

[28] V. Carlan *et al.*, "Toward implementing a fully automated truck guidance system at a seaport: Identifying the roles, costs and benefits of logistics stakeholders," *J. Shipping Trade*, vol. 4, no. 1, pp. 1–24, 2019.

[29] K. A. Khaliq, A.Qayyum, and J.Pannek, "Methodology for development of logistics information and safety system using vehicular adhoc networks," *Dynamics in Logistics*. Berlin, Germany: Springer, Cham, 2017, 185–195.

[30] C. S. Lalwani, "Wireless vehicular networks to support road haulage and port operations in a multimodal logistics environment," *Proc. IEEE/INFORMS Int. Conf. Serv. Operations, Logistics Inform.*, 2009, pp. 62–67.

[31] W. F. Silvanoand R.Marcelino, "Iota tangle: A cryptocurrency to communicate Internet of Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, 2020.



ANDREA TESEI received the master's degree in computer science and networking jointly from the Sant'Anna School of Advanced Studies and the University of Pisa, Pisa, Italy in 2017. He is currently working toward the Ph.D. degree with the Department of Information Engineering, University of Pisa. Since January 2018, he has been with the National Inter-University Consortium for Telecommunications, Pisa, Italy, as a Researcher. His research interests include vehicular public key infrastructure, security schemes for intelligent transportation systems, vehicle revocation mechanisms, and misbehavior detection.

DOMENICO LATTUCA received the master's degree in telecommunications engineer from the University of Palermo, Palermo, Italy, in 2018. He is currently working toward the Ph.D. degree in the Department of Information Engineering at the University of Pisa, Pisa, Italy. Since February 2019, he has been with the National Inter-University Consortium for Telecommunications, Pisa, Italy, as a Researcher. His research interests include vehicular misbehavior detection, machine learning, and security mechanisms for intelligent transportation system.

ALEXANDR TARDO received the master's degree in telecommunications engineering from the University of Catania, Catania, Italy, in 2015. He is currently a Senior Research and Project Manager with the National Inter-University Consortium for Telecommunications leading R&D activities as a Member of JLAB-Ports. His research interests include ICT infrastructures, microservices architectures, IoT, digitalization of processes, digital twins, and disruptive and cutting-edge technologies applied to the logistics domain in seaports.

LUCA DI MAURO received the bachelor's degree in computer science from the University of Pisa, Pisa, Italy, in 2016. He joined the Networks of Embedded Systems area, National Inter-University Consortium for Telecommunications, Pisa, Italy, as a Vehicular Communication and IoT Researcher working in the AUTOPILOT project in 2017. He is currently a Researcher with the Sant'Anna School of Advanced Studies, Pisa, Italy, to develop applications for the road safety of vulnerable users in a smart city environment. His research interests have a specific focus on C-ITS systems, wireless sensor networks, and embedded systems.

PAOLO PAGANO received the master degree in IT from the Sant'Anna School of Advanced Studies, Pisa, Italy and the Ph.D. degree in high energy physics from Trieste University, Trieste, Italy, having worked for the COMPASS collaboration at CERN. Since 2009, he has been with the National Inter-University Consortium for Telecommunications (CNIT), Pisa, Italy, leading the Networks of Embedded Systems area, the National Laboratory of Photonic Networks and Technologies, Pisa, Italy. Since October 2015, he has been the Director of the joint (CNIT / Port Network Authority of the Northern Tyrrhenian Sea) laboratory on advanced sensing and networking in sea ports. He has coauthored about 100 peer reviewed papers to international journals and conferences. His research focuses on ITS and Port of the Future. He is participating (on behalf of CNIT) to the ETSI standardization committees for Cooperative ITS and maritime communication. Since September 2018, he has been a Member of the Working Group "Smart Roads", Technical Committee on Autonomous Driving at the World Road Association.

MARCO LUISE is a Full Professor of telecommunications with the University of Pisa, Pisa, Italy. He has chaired a number of scientific conferences, including EUSIPCO 2006 and IEEE ICASSP in 2014. He was the Editor of the IEEE TRANSACTION COMMUNICATION, currently the Co-Founder of the *International Journal of Navigation and Observation*, the Division Editor of the *Journal of Communication and Networks*, and was the Coordinator of the *European Network of Excellence in Wireless Communications.* He has authored more than 300 publications, and his main research interests include the broad area of wireless or satellite communications and positioning.

PAULO C. BARTOLOMEU received the Ph.D. degree in informatics engineering from the University of Aveiro, Aveiro, Portugal, in 2014. He has participated in several R&D projects both at the academias, which include ARMONIO, CAMBADA and Smart Green Homes and in the industries which include CIRaF, DHT-Mesh, BikeEmotion, Living Usability Lab, SheepIT. He is the author of two patents and more than 40 scientific publications including papers in conferences, journals and book chapters. He is currently an invited Adjunct Professor with the University of Aveiro and a Senior Researcher with the Instituto de Telecomunicações, Aveiro, Portugal, working on an industry joint project named EV4Energy. His research interests include real-time communications, blockchain/DLT, SSI, and IoT.

JOAQUIM FERREIRA received the Ph.D. degree in informatics engineering from the University of Aveiro, Aveiro, Portugal, in 2005. He is currently an Adjunct Professor with the School of Technology and Management, University of Aveiro and a Researcher with Telecommunications Institute. He has been involved in several international and national research projects. He is the author of several scientific papers and book chapters in his areas of expertise. His research interests include dependable distributed systems, fault-tolerant real-time communications, wireless vehicular communications, cooperative ITS systems, and medium access control protocols. He was on a several scientific committees of conferences.