Cybersecurity in the Transportation Sector: Closing the Revocation Gap in the European Smart Tachograph

Teodor CĂLUGĂRU, Constantin-Sebastian LAZĂR , Aurel-Alberto URSACHE
[1]Doctoral School of Entrepreneurship, Business Engineering and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania
teodor.calugaru@stud.fsa.upb.ro, constantin.lazar98@stud.acs.upb.ro, aurel.ursache@stud.faima.upb.ro

Abstract: Modern European smart tachograph infrastructures rely on Elliptic Curve Cryptography and Advanced Encryption Standard primitives to enforce data authenticity and operational security. However, certificates are verified statically, so a compromised credential remains trusted until it expires. This paper discusses these challenges in transportation networks and proposes a lightweight extension to the existing public key infrastructure that keeps the same trusted authorities while dynamically verifying the revocation status of the certificates involved. An initial software implementation shows that the exposure period of a compromised certificate is reduced from the remaining validity period, up to thousands of days, to the status-update interval.
Keywords: Smart Tachograph, Operational Technology Security, Trust Infrastructure, Public Key Infrastructure, Revocation Gap.

INTRODUCTION

Modern transportation systems have evolved from electromechanical assemblies into extremely interconnected Cyber-Physical Systems (CPS). The integration of onboard processing units (Electronic Control Units – ECUs), sensor networks, and wireless communication channels has enabled real-time fleet management, automated telemetry, and enhanced road safety. However, this new infrastructure represents a broad attack surface for malicious actors, exposing operational assets to cyber threats that threaten both data confidentiality and physical vehicle safety and public security.

In Industrial Control Systems (ICS) and Operational Technology (OT) deployed within regulated transport, Public Key Infrastructures (PKIs) serve as the foundation of digital trust, authentication, and non-repudiation. Historically, cryptographic

https://doi.org/10.54851/v8i2y202607

architectures for embedded devices in regulatory frameworks have relied on static trust models: strong cryptographic algorithms and key sizes evaluated periodically, paired with rigid credential lifecycle management (European Parliament & Council of the European Union, 2014).

This paper focuses on regulated commercial road transport, examining the European Smart Tachograph (Generation 2) security framework. While the system successfully modernized its cryptographic primitives by transitioning to Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) (European Commission, 2016), its underlying trust model exhibits a structural vulnerability: the absence of a dynamic credential revocation mechanism (European Commission Joint Research Centre, 2018). Equipment credentials validated entirely offline rely on trust anchors and certificates with extended lifetimes, spanning up to several decades (European Root Certification Authority, 2021). Consequently, if a private key is compromised, the associated credential remains cryptographically valid and operationally trusted until its expiration.

To asses whether the periodic modernization of the cryptographic algorithms is sufficient to maintain a secure environment, this paper examines the limitations of static trust models. The *When Bits Attack Steel: OT/ICS Security in Transportation* and *Spoofing the Signal: GNSS and Wireless Vulnerabilities* sections explore the security paradigms of OT and ICS, including wireless and Global Navigation Satellite Systems (GNSS) vulnerabilities. The *The Weakest Link: Supply Chain and Third-Party Risk* and *Racing Against the Rulebook: Regulation and Governance* sections investigate supply chain risks associated with embedded systems, as well as regulatory and governance challenges. The *Research Methodology* section outlines the research methodology, while the *Trust Infrastructure of the European Smart Tachograph* section describes the trust infrastructure of the European Smart Tachograph. The paper presents the proposed architecture and its practical demonstration in the *Proposed Architecture and Practical Demonstrations* section, followed by its quantitative evaluation in the *Quantitative Evaluation* section. The *Security Analysis and Comparison with Existing Revocation Mechanisms* section analyzes the security of status distribution and compares the proposed approach with existing revocation mechanisms. Finally, the Conclusions section summarises the main findings and contributions of the paper.

WHEN BITS ATTACK STEEL: OT/ICS SECURITY IN TRANSPORTATION

OT in transportation environments operates under requirements fundamentally distinct from enterprise Information Technology (IT). While traditional IT systems prioritize the confidentiality of data according to the classic confidentiality, integrity and availability (CIA) triad, OT and ICS environments place primary emphasis on availability, physical safety, and real-time determinism. A successful cyber-physical attack on transportation infrastructure extends far beyond data exfiltration; it interacts directly with physical mechanics ("bits attacking steel"), potentially inducing physical disruptions, signal tampering, or dangerous overrides of vehicular control systems (Chothia et al., 2017).

Across the rail, aviation and automotive sectors, the adoption of Internet Protocol (IP)-based protocols and commercial wireless networks for telemetry and diagnostics has ended the air gap between these industries. For instance, the introduction of the Global System for Mobile Communications – Railway (GSM-R) and the Future Railway Mobile Communication System (FRMCS) into the European Rail Traffic Management System (ERTMS) for the rail industry created potential security threats from jamming, spoofing and sending unauthorized messages into these systems (Chothia et al., 2017). Also,

the integration of passenger In-Flight Entertainment (IFE) systems with the avionics systems of commercial airliners through Avionics Full-Duplex Switched Ethernet (AFDX/ ARINC 664) introduces extra attack surfaces against the aircraft's communications systems (Mancuso, Louis & Caccamo, 2015).

In the area of road transport, the two technologies converge in the use of Vehicle Units (VUs) and sensors on those vehicles. Vehicles that weigh over 3.5 tonnes are required by law to have certain electronic elements embedded into their construction; vehicles used for the carriage of passengers that can carry more than nine persons including the driver are also subject to these rules (European Parliament & Council of the European Union, 2014). Unlike computer software, which is frequently updated to prevent security breaches, the software that manages these units and sensors has a lifespan of around 10-15 years during which it must remain compliant with existing regulations. Updating firmware or administrative credentials on these devices introduces severe operational and regulatory friction:

- Regulatory Recertification: Any change to the certified software baseline requires recertification of that software from accredited national testing laboratories under Common Criteria Protection Profiles (e.g., BSI-CC-PP-0094-V2) (Bundesamt für Sicherheit in der Informationstechnik, 2021).
- Intermittent Connectivity: The connectivity in commercial fleets is intermittent and constrained. The areas in which they operate have varying levels of cellular coverage. Also, the Dedicated Short-Range Communications (DSRC) channels that are utilized for the enforcement of traffic regulations have a limited bandwidth, which makes it difficult to distribute the security updates for those vehicles (Bundesamt für Sicherheit in der Informationstechnik, 2021).
- Offline Trust Assumption: The system design requires that the credentials of each vehicle are verified 100% offline during roadside inspections, eliminating the need for any real-time connection to the central databases of the agency in question (European Commission, 2016).

If an embedded device or driver card is physically or logically compromised (e.g., through hardware fault injection or side-channel extraction), the private key material of the device will be exposed (Kocher, Jaffe & Jun, 1999). Since the operational technology system uses the certificate chain and timestamp as indicators of a valid certificate, a compromised certificate will still be able to generate telemetry data, logs and rest periods without detection (European Parliament & Council of the European Union, 2014). So, implementing only strong algorithms will fail to prevent unauthorized access to the network if there is no method of propagating invalid certificates throughout the disconnected nodes.

SPOOFING THE SIGNAL: GNSS AND WIRELESS VULNERABILITIES

Modern transport increasingly relies on GNSS, and their widespread use has also increased exposure to two main classes of attack. Jamming floods the receiver with noise until it can no longer track the satellite signal, whereas spoofing feeds it counterfeit signals that alter the computed position, velocity and time while the device appears to operate normally. Of the two, spoofing is the more dangerous, because it is far harder to recognize than ordinary jamming (Dułowicz, Skokowski & Kelner, 2026).

These vulnerabilities are no longer confined to theory, as they have already become visible in practice. In June 2017, more than twenty vessels near the Russian port of Novorossiysk in the Black Sea reported positions roughly 25 nautical miles away from their actual location, in some cases inland, an anomaly attributed to suspected Global Positioning System (GPS) spoofing (U.S. Maritime Administration, 2017;

Inside GNSS, 2017). More broadly, aviation authorities report a sharp rise in GNSS interference affecting airports and flight operations (European Union Aviation Safety Agency, 2024), and in road freight, criminals have used jamming devices to disable the trackers of trucks and cargo in theft and hijacking cases (CCJ, n.d.).

Neither attack can be ruled out entirely, but both can be mitigated through defences organised in several layers (Sony Semiconductor Solutions Group, 2025). At the receiver level, relying on several constellations (for instance Galileo and GPS) and several frequency bands (such as L1 and L5) makes it possible to cross-check the incoming signals and flag the inconsistencies that typically betray a spoofing attempt. A second layer is cryptographic authentication of the navigation message itself, as offered by Galileo Open Service Navigation Message Authentication (OSNMA). These measures are directly relevant to road transport, since the second version of the smart tachograph is required to authenticate Galileo signals through OSNMA (European Commission, 2021). Authenticated positioning, however, protects only the data entering the tachograph; it does not guarantee that the equipment and cards which record and sign these data can still be trusted, which is the question addressed in the remainder of this paper.

THE WEAKEST LINK: SUPPLY CHAIN AND THIRD-PARTY RISK

Transportation networks, from container ports to airline reservation systems to freight-rail control centers, are among the most externally dependent critical infrastructures in the modern economy, which makes transportation an emblematic case of the "weakest link" problem in cybersecurity. Ghadge et al. (2020), in a systematic literature review of cyber risk in supply chains, argue that risk cannot be assessed at the level of a single firm because every node and connection in a network is a potential point of failure, and that cyber risk propagates outward from its point of origin through a "cascading or ripple effect," concluding that "a chain is only as strong as its weakest link". This dynamic is especially acute in transportation, where a single shipment moves through a multimodal chain connecting manufacturers, terminal operators, customs authorities, freight forwarders and last mile carriers, each running separate, often poorly integrated IT systems.

Clavijo Mesa, Patino-Rodriguez and Guevara Carazas (2024), in a systematic review of 110 journal articles on maritime cybersecurity, find that distributed denial-of-service attacks and malware are the top concerns across maritime supply chain stakeholders, and that vendors, contractors, and even port officials connecting external devices to onboard or terminal systems represent a significant source of third-party exposure.

Aviation supply chains present a comparable exposure through a different mechanism: an intricate web of manufacturers, software vendors, airlines, airport authorities, and ground-handling contractors, each a potential point of entry. Mizrak and Akkartal (2024) suggest that in aviation, unlike in less regulated sectors, third-party risk is best mitigated not only through technical controls but through compliance regimes that bind vendors, maintenance contractors, and airport operators to a common security baseline.

Rail systems face a parallel challenge as signaling, traffic management, and freight-tracking systems are increasingly digitized and interconnected. Abudu et al. (2025), in a systematic bibliometric review of 70 articles on rail cybersecurity, find that digitalization of rail freight has expanded the sector's attack surface faster than its cybersecurity governance has matured.

Road freight and cross-border logistics illustrate how third-party risk compounds across organizational boundaries rather than within a single firm. Urciuoli et al. (2013), studying cyber security threats in cross-border transport and logistics chains, describe how ill-secured connections between

customs authorities, freight forwarders, and carriers function as points of penetration that can be exploited to manipulate cargo data, transportation schedules, and customs declarations. Because road and multimodal logistics chains depend on continuous data exchange between public authorities and private operators of varying digital maturity, the weakest link in this segment is often not a single vendor but the handoff points between otherwise well-defended organizations.

The tachograph system likewise involves multiple stakeholders. Vehicle units, motion sensors, and cards are manufactured by distinct vendors and certified by national authorities, subsequently passing through workshops, enforcement authorities, and transport operators. Consequently, a private key can be compromised at any point along this chain, long before the certificate's expiration. A mechanism to revoke an individual certificate is therefore a critical requirement, and the *Trust Infrastructure of the European Smart Tachograph* section demonstrates that the current infrastructure does not yet incorporate such a mechanism.

RACING AGAINST THE RULEBOOK: REGULATION AND GOVERNANCE

Regulation in the transportation sector has historically followed major incidents rather than anticipated them, and Europe's Network and Information Security Directive (NIS2) shows how a single harmonizing rule can still fragment once it meets sector reality. Wachnik (2025) finds that while the directive sets a common baseline, each mode applies it through different sectoral guidance, reporting channels, and pre-existing safety cultures, producing convergent legal obligations but divergent day-to-day practice. The result is less a single rulebook than a family of overlapping ones, each moving at its own pace.

Maritime governance illustrates how far a regulator can lag behind a fast-moving threat. Karim (2022), analyzing the International Maritime Organization's legal instruments, finds that the International Maritime Organization (IMO)'s principal response, its non-mandatory Guidelines on Maritime Cyber Risk Management, folds cyber risk into existing safety management systems rather than creating binding, cybersecurity-specific obligations, leaving flag states and shipowners considerable discretion over implementation.

Aviation has moved further toward binding regulation, but coordination across governance layers remains an open problem. Metin, Dümer and Wynn (2026), interviewing senior industry practitioners to validate a governance-risk-compliance framework for airport cybersecurity, find that the sector's vulnerabilities are driven less by any single missing technical control than by fragmented oversight, uneven vendor accountability, and unclear lines of responsibility.

Rail regulation shows the same pattern at a starker scale. Oka, Hromada and Jasek (2026), studying how European critical rail infrastructure operators are adopting NIS2, identify governance fragmentation, uneven cybersecurity maturity between IT and legacy operational technology, and supplier dependency as the sector's core compliance obstacles.

In the domain of road transport, the tachograph constitutes a strictly regulated device, mandated by Regulation (EU) No 165/2014 (European Parliament & Council of the European Union, 2014). While its technical specifications, laid down in Commission Implementing Regulation (EU) 2016/799, Annex IC, Appendix 11 (European Commission, 2016), specify the cryptographic algorithms to be used in detail, they do not define a certificate revocation mechanism, an omission that is analyzed in the *Trust Infrastructure of the European Smart Tachograph* section.

RESEARCH METHODOLOGY

The methodology of the present study relies on a conceptual analysis of an operational trust infrastructure, combined with an applied prototype designed for the functional validation of the proposed solution.

The conceptual analysis examines the PKI of the European smart tachograph, drawing upon the applicable regulatory and technical framework: Regulation (EU) No 165/2014 (European Parliament & Council of the European Union, 2014), Commission Implementing Regulation (EU) 2016/799, Annex IC, Appendix 11 (European Commission, 2016), the European Root Certification Authority (ERCA) Certificate Policy (European Commission Joint Research Centre, 2018), and its published reference set of keys and certificates (European Commission Joint Research Centre, n.d.). This framework is complemented by domain literature describing the design decisions and trade-offs made in defining the system (Baldini et al., 2018). The analysis focuses on three key dimensions: the hierarchy structure of certification, the underlying cryptographic primitives, and the lifecycle management procedures for credentials. The objective of this phase is to identify the gap between the update pace of the cryptographic primitives and the maturity level of the trust model.

The applied component consists of a software prototype that functionally reproduces the validation process of an equipment credential under two distinct configurations. The first configuration corresponds to the current model, in which the acceptance decision relies exclusively on the offline verification of the certification chain up to a pre-installed trust anchor, along with the validity period check. The second configuration extends this process by incorporating an additional step to query the credential status, without modifying the existing chain validation. The three-level certification hierarchy is effectively generated within the prototype using elliptic curve cryptography (National Institute of Standards and Technology, 2023), and the validation decisions are genuinely computed by the implementation rather than simulated.

The comparative evaluation is conducted across eight synthetic scenarios (S1–S8), described in the *Proposed Architecture and Practical Demonstrations* section. The first four model the functional behavior of the two configurations: the presentation of a legitimate credential, the presentation of a credential issued outside the recognized hierarchy, the presentation of a legitimate credential reported as compromised while still within its validity period, and the evolution of the time window between the compromise event and the actual rejection, as a function of the status information update frequency. The remaining four model attacks against and failures of the status distribution: a forged status list, the replay of an older genuine list, the unavailability of updates after a revocation, and blocked updates, which reveal the trade-off between the exposure window and the rejection of legitimate credentials. For S1–S4, the validation decision is recorded under both configurations, and for S4 the resulting exposure window is quantified; S5–S8 apply only to the proposed configuration, since the current model does not use a status list.

The methodological limitations are explicitly acknowledged. The prototype serves as a functional validation in a controlled environment rather than a performance evaluation under operational conditions. Type-approved equipment was not used; the memory footprint and response time of the proposed solution were measured on a general-purpose computer, as presented in the *Quantitative Evaluation* section , while its behavior on embedded components, including power consumption, falls outside the scope of this evaluation. The attack scenarios are modeled at the trust model and credential management levels, without reproducing operational exploitation techniques. The obtained results do not substitute the formal security certification process mandated for regulated transport equipment.

TRUST INFRASTRUCTURE OF THE EUROPEAN SMART TACHOGRAPH

The tachograph constitutes a mandatory piece of equipment for commercial vehicles exceeding 3.5 tonnes and for passenger

transport vehicles capable of carrying more than nine persons including the driver (European Parliament & Council of the European Union, 2014), playing a vital role in recording drivers' driving and rest times, as well as serving as an enforcement tool for social and road safety legislation. Naturally, security measures play a critical role in the described system, as data falsification can lead to fatigued drivers behind the wheel or unfair competition among operators (given that an operator manipulating the tachograph can compel drivers to exceed legal limits, thereby yielding more trips and higher revenue) (Baldini et al., 2018).

Figure 1 illustrates the organization of the infrastructure responsible for validating tachograph equipment credentials, structured into two distinct stages: certificate issuance and in-service verification. ERCA serves as the European-level component, generating the root key pair and signing the certificates of National Authorities (European Commission Joint Research Centre, 2018). At the Member State level, each National Authority acts as a Member State Certification Authority (MSCA) and specializes according to the type of equipment served: MSCA_Card issues certificates for tachograph cards, whereas MSCA_VU-EGF issues certificates for vehicle units and External GNSS Facilities (EGF) (European Root Certification Authority, 2021). The lower tier of the hierarchy comprises the actual equipment, with each unit receiving a certificate issued by the corresponding National Authority. The root certificate is pre-installed in every piece of equipment to serve as a trust anchor (European Commission, 2016). The verification stage is performed locally within the equipment. Upon the presentation of a credential, it is validated by reconstructing the certification chain up to the pre-installed trust anchor, followed by the verification of its validity period.

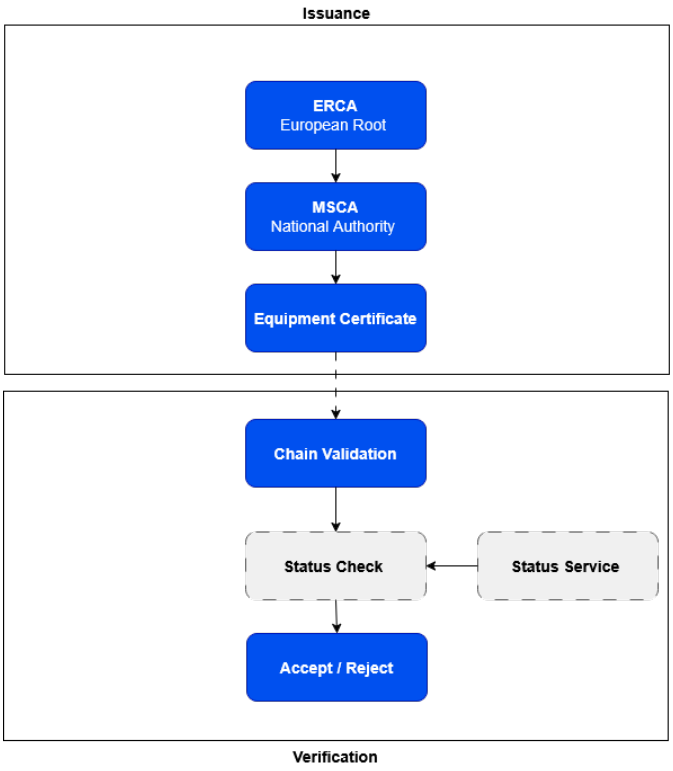


Figure 1. *Smart tachograph trust hierarchy and the proposed status verification step*

These validation steps produce a result that determines the acceptance or rejection decision. Elements depicted with dashed lines are not part of the current architecture but rather represent the extension proposed in the *Proposed Architecture and Practical Demonstrations* section.

The second generation of the system updated the underlying cryptographic primitives, replacing 1024-bit Rivest-Shamir-Adleman (RSA) keys with 256-to-521-bit elliptic curve cryptography and the Triple Data Encryption Standard (3DES) with 128-to-256-bit AES (European Commission, 2016). The certificates do not use the standard X.509 format, but rather a compact card-verifiable format chosen to reduce the memory and processing requirements of embedded components (European Commission, 2016). Upon inserting a card into the vehicle unit, the two entities perform mutual authentication: each presents its own certificate and proves possession of the corresponding private key, after which both independently derive the same session keys, subsequently used to protect the data exchange (European Commission, 2016). From an algorithmic standpoint, the system is thus aligned with current best practices. The observations that follow do not target the cryptographic primitives themselves, but rather the trust model in which they are deployed.

Table 1. *Digital certificates validity periods in the smart tachograph PKI*

Certificate	Validity
ERCA root	34 years 3 months
MSCA	7 to 17 years
Vehicle Unit	15 years 3 months
Driver Card	5 years 1 month

The certificates issued within this hierarchy have the validity periods presented in Table 1. These duration parameters are sized according to the physical equipment lifecycle rather than the evolving threat landscape: a vehicle unit certificate spans over 15 years, while that of the European Root Certification Authority covers 34 years (European Root Certification Authority, 2021). Furthermore, the verification of these certificates is performed exclusively locally, at the equipment level, as previously described. A major vulnerability lies in the fact that the system does not provide a Certificate Revocation List (CRL) or a status querying service. Consequently, a credential reported as compromised remains valid until its natural expiration date. Coupled with the durations detailed in Table 1, this implies that the administrative revocation of a card fails to propagate to operational equipment for years on end.

PROPOSED ARCHITECTURE AND PRACTICAL DEMONSTRATIONS

Although the current model validates the certification chain and the validity period locally, it nevertheless exhibits a major architectural flaw: a compromised credential cannot be rejected prior to its expiration. To address this, the architecture proposed in this paper introduces a credential status verification layer superimposed on the existing validation mechanism without altering it. A status service operated at the National Authority level periodically publishes a signed list of revoked credentials, which is distributed to the equipment via existing system channels and stored locally by each unit. The digital signature applied to this list prevents the insertion of forged versions.

Each status list contains three additional mandatory fields: the issuance date, the expiration date (defining the next scheduled update), and a sequence number that increments with each publication. The digital signature covers all these fields in addition to the list of revoked certificates. Upon receiving a new list, the unit performs the following checks, ordered from the least to the most computationally expensive: the list must not exceed a maximum size, its sequence number must be strictly greater than that of the list currently stored, its issuance date must not

lie in the future, and its digital signature must be valid. Only when all four checks succeed is the stored list replaced by the new one; otherwise, the new list is discarded, and the stored one is kept. Thus, a list is verified only once, upon receipt, rather than during every certificate validation.

The certification chain validation remains unchanged: the same hierarchy, the same certificates, and the same verification process up to the pre-installed root anchor. Three checks are added following the successful validation of the chain, in the following order: verifying the authenticity of the stored list (its digital signature must be valid; since the stored list changes only when an update is accepted, the result of the signature check performed upon receipt can be reused), checking the freshness of the list (the verification date must fall between its issuance date and its expiration date), and finally, verifying that the certificate does not appear in the status list. If the stored list has expired, the credential is rejected; the implications of this choice are discussed in the *Security Analysis and Comparison with Existing Revocation Mechanisms* section. This design choice avoids modifying an already type-approved safety mechanism, adding protection as an independent layer. The validation logic for both models is presented in the following sequence:

```
def validate_chain(equipment, msca, erca, at):
    if not verify_signature(equipment, msca.public_key):
        return Decision(False, "equipment not issued by a known MSCA")
    if not verify_signature(msca, erca.pub):
        return Decision(False, "MSCA not signed by trusted root")
    for c in (equipment, msca):
        if not (c.not_before <= at <= c.not_after):
            return Decision(False, "outside validity period")
    return Decision(True, "chain valid")

def validate_with_status(equipment, msca, erca, status, status_pub, at):
    base = validate_chain(equipment, msca, erca, at)
    if not base.accepted:
        return base
    if not verify_signature(status, status_pub):
        return Decision(False, "status list signature invalid")
    if not (status.issued_on <= at <= status.next_update):
        return Decision(False, "status list not fresh")
    if equipment.subject in status.revoked:
        return Decision(False, "credential revoked")
    return Decision(True, "chain valid, not revoked")

def accept_status_update(current, new, status_pub, at):
    if len(new.revoked) > MAX_ENTRIES:
        return current                          # oversized list discarded
    if current and new.serial <= current.serial:
        return current                          # replay / rollback discarded
    if new.issued_on > at:
        return current
    if not verify_signature(new, status_pub):
        return current                          # forged list discarded
    return new                                  # list accepted and cached

# on receipt of a new status list (update event)
stored = accept_status_update(stored, received, status_pub, today)

# on every credential presentation (e.g., card insertion)
decision = validate_with_status(card, msca, erca, stored, status_pub, today)
```

The two functions are invoked at different moments: `accept_status_update` when a new status list is received and `validate_with_status` at every credential presentation, using the list stored by the former. The signature check in `validate_with_status` is shown for completeness; in practice, it is performed once in `accept_status_update`, and only the freshness and membership checks are repeated at each validation. The cost of both variants is quantified in the *Quantitative Evaluation* section.

The two models were comparatively evaluated across eight scenarios, using a three-level certificate hierarchy and elliptic curve cryptography. The first scenario (S1) involves a legitimate credential within its validity period, which is accepted by both models. In the second scenario (S2), both models behave identically by rejecting a credential issued outside the recognized hierarchy during the certification chain validation stage, thereby confirming that the proposed layer does not weaken the baseline protection of the existing module. The third scenario (S3) presents a contrasting case: a legitimate and valid credential that has been reported as compromised is accepted by the current model, but rejected by the proposed one (both models operate on identical cryptographic material and yield opposing outcomes, with the discrepancy arising solely from the revocation information). The execution results of the prototype demonstrating the eight scenarios are presented below:

```
SMART TACHOGRAPH TRUST MODEL - VALIDATION SCENARIOS
--- S1 legitimate credential ---
  (A) current: ACCEPT - chain valid and within validity period
  (B) proposed: ACCEPT - chain valid, within validity period, not revoked
--- S2 credential issued outside the recognized hierarchy ---
  (A) current: REJECT - MSCA certificate not signed by trusted root
  (B) proposed: REJECT - MSCA certificate not signed by trusted root
--- S3 legitimate credential reported compromised (still within validity) ---
  (A) current: ACCEPT - chain valid and within validity
  (B) proposed: REJECT - credential revoked per status list
  -> identical crypto, opposite outcome: revocation is the only difference
--- S4 exposure window vs. status refresh interval ---
  credential compromised on: 2026-03-10
  natural expiry (model A): 2030-12-31
  exposure, model A: 1757 days (until expiry)
  exposure, model B (refresh 1d): <= 1 day
  exposure, model B (refresh 7d): <= 7 days
  exposure, model B (refresh 30d): <= 30 days
  exposure, model B (refresh 90d): <= 90 days
--- S5 forged status list presented to the device ---
  update handling: update rejected: invalid signature
  (B) proposed, forged list used directly: REJECT - status list signature invalid
--- S6 replay of an older genuine list (rollback attempt) ---
  update handling: update rejected: serial not newer (rollback/replay)
  (B) proposed, caught list kept: REJECT - credential revoked per status list
--- S7 status updates unavailable after revocation (suppression) ---
  day + 3: ACCEPT - chain valid, within validity period, not revoked
  day + 7: ACCEPT - chain valid, within validity period, not revoked
  day + 8: REJECT - status list not fresh
  day +30: REJECT - status list not fresh
--- S8 updates blocked: exposure vs. lockout of legitimate credentials ---
  list validity 1 d: compromised card accepted until day +1, legitimate card rejected
from day +2
  list validity 7 d: compromised card accepted until day +7, legitimate card rejected
from day +8
  list validity 30 d: compromised card accepted until day +30, legitimate card rejected
from day +31
  list validity 90 d: compromised card accepted until day +90, legitimate card rejected
from day +91
```

The fourth scenario (S4) illustrates the exposure window, defined as the time interval between the moment a credential is compromised and the point at which it effectively ceases to be accepted. In the current model, this interval extends until the natural expiration of the certificate (1757 days for the analyzed credential). Conversely, under the proposed model, the exposure is bounded by the update interval of the list, being reduced to at most 90, 30, 7, or 1 day(s) (Figure 2). Thus, narrowing this time window does not require modifying the cryptographic primitives or the chain validation, but simply adding the status list. Scenarios S5 to S8 address attacks against the status distribution and the unavailability of updates; they are discussed in the *Security Analysis and Comparison with Existing Revocation Mechanisms* section.

While the proposed model does not entirely eliminate the exposure, it binds it to the update interval. The evaluation was conducted in a controlled environment across synthetic scenarios, without validation on type-approved equipment.

QUANTITATIVE EVALUATION

The *Proposed Architecture and Practical Demonstrations* section demonstrated the functionality of the proposed mechanism; this section evaluates its performance overhead. Specifically, four metrics were measured: certificate validation time, list update cost (i.e., verification of the new list upon receipt), list size, and the memory footprint occupied by the list. These measurements were evaluated as a function of the number of revoked certificates in the list (N = 100, 1,000, 10,000, and 100,000), utilizing the prototype implementation described in The *Proposed Architecture and Practical Demonstrations* section, which employs Elliptic Curve Digital Signature Algorithm (ECDSA) signatures over the P-256 curve with the Secure Hash Algorithm (SHA-256) hash function). Each reported value represents the median of 31 execution runs. Benchmark measurements were conducted on a Dell Precision 7670 laptop equipped with an Intel Core i7-12850HX processor (2.10 GHz) and 32 GB of RAM, running Windows 11 (25H2), Python 3.13.14, and the cryptography library (version 49.0.0). The implications of using a general-purpose host system rather than an embedded device are discussed at the end of this section.

While the current model validates a certificate (verifying the signature chain and validity period) in 0.115 ms, independently of N (as it does not use the status list), the proposed model's validation time increases with the list size when verifying the list's signature at

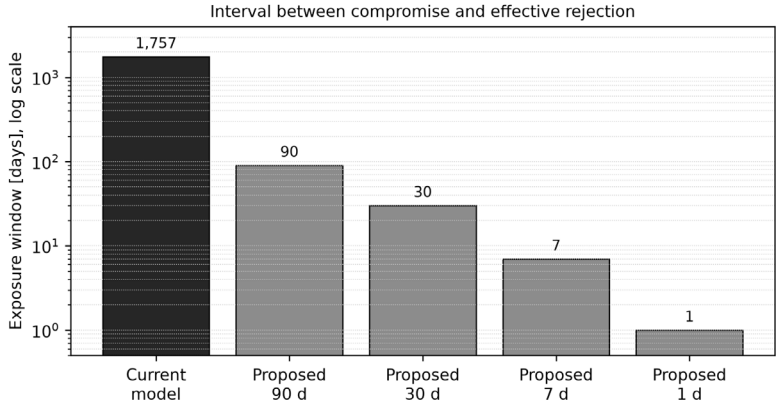


Figure 2. *Exposure window: current model vs. proposed status refresh interval*

every validation, rising from 0.173 ms for N = 100 to 24.089 ms for N = 100,000 (Figure 3a). This overhead stems from the requirement to process the entire list at each validation. Conversely, when the list is verified only once upon receipt and subsequently stored, validation takes between 0.116 ms and 0.117 ms across all values of N, rendering it practically identical to the current model. Under this strategy, each validation only requires verifying the list's freshness and performing a membership lookup, both of which incur negligible overhead. Consequently, if the list is verified upon receipt, checking for revocation introduces virtually no additional cost during certificate validation, regardless of the list size, thereby supporting the design decision presented in the *Proposed Architecture and Practical Demonstrations* section.

When the list is verified upon receipt, the verification cost shifts from validation to a single occurrence during the update process. This update verification ranges from 0.057 ms (N = 100) to 24.026 ms (N = 100,000), as represented by the dashed line in Figure 3a. The list size scales linearly with N, at approximately 20 bytes per revoked certificate, growing from 2.1 kB (N = 100) to 2.0 MB (N = 100,000), as shown in Figure 3b. Regarding the memory footprint, the prototype consumes 10.2 MB for N = 100,000; however, this value is inflated by Python's internal data structures, whereas a compact storage layout on an embedded device would be expected to yield a memory footprint much closer to the transmitted size. Thus, for large lists, the practical bottleneck is not computational overhead but rather the size of the list that must be transmitted, a factor particularly relevant for low-bandwidth channels such as DSRC, as mentioned in the *When Bits Attack Steel: OT/ICS Security in Transportation* section.

One potential denial-of-service (DoS) scenario involves flooding the device with numerous forged lists to keep the processor fully occupied with their verification. First, replayed old lists and lists exceeding the size limit are rejected in under 1 µs, as they are filtered out prior to signature verification. A forged list with a new sequence number, however, cannot be rejected until its signature is fully verified; for N = 100,000, this operation takes 22.5 ms, meaning the device can reject at most approximately 44 maximum-size forged lists

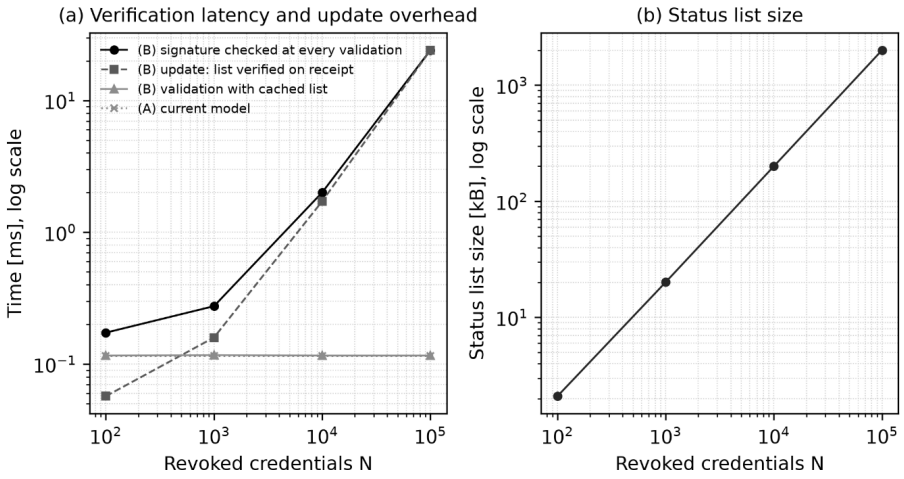


Figure 3. *Cost of the status check as a function of the number of revoked certificates: (a) validation time and update cost; (b) status list sizep*

per second (Table 2). Moreover, the size limit caps the maximum cost of a single list, while transmitting 44 lists of 2 MB per second would require an attacker to use a channel of approximately 700 Mbit/s, far exceeding the capacity of the low-bandwidth channels available to the tachograph, such as DSRC, as discussed in the *When Bits Attack Steel: OT/ICS Security in Transportation* section. Even if verification on an embedded device were two orders of magnitude slower, saturating the processor would still require approximately 7 Mbit/s. In conclusion, DoS attacks based on flooding with forged lists are constrained by the communication channel rather than the processor.

Absolute values were measured on a general-purpose computer, meaning that execution times are expected to be higher on an actual tachograph. Nevertheless, the relative performance behavior is expected to generalize, as it is dictated by the algorithmic structure rather than the underlying platform. Specifically, with the list verified exclusively upon receipt, validation incurs a cost comparable to the current model, supplemented only by a freshness check and a membership lookup, while the update cost and list size scale proportionally with N. On a resource-constrained device, the primary cost factors are the number of revoked certificates in the list, the update frequency, and the communication channel bandwidth, rather than the processing power required for validation. Measurements on type-approved hardware or a secure element were not feasible, as such specialized hardware is not accessible to an academic laboratory, and remains a subject for future work.

SECURITY ANALYSIS AND COMPARISON WITH EXISTING REVOCATION MECHANISMS

The security of the proposed mechanism rests upon several assumptions, which are detailed below. The most critical assumption concerns the key held by the status service of the MSCA, which is used to digitally sign the list. Its public key must reach the tachograph through a trusted path, either pre-installed alongside the ERCA root or certified within the existing hierarchy. In the event of a private (signing) key compromise, an attacker could publish forged lists; hence, this key must be protected with the same rigor as a certification authority key. Furthermore, the distribution channels (DSRC, workshop cards, ITS-G5 links for Intelligent Transport Systems) are assumed to be untrusted, meaning security must not rely on them, but rather on the digital signature, the sequence number, and the list's freshness. Additionally, the tachograph's internal clock plays a crucial role, as list freshness is evaluated against internal time. It is therefore assumed that an attacker cannot manipulate the clock, an assumption already embedded in the current system, given that the tachograph inherently relies on its internal clock to record driving times. Moreover, the tachograph's storage must be secured to prevent any unauthorized modification of the list once verified and saved. Lastly, system security naturally relies

N	Forged list: rejection time	Forged lists rejected per second	Replayed or oversized list: rejection time
100	0.058 ms	17,241	< 1 µs
1,000	0.346 ms	2,888	< 1 µs
10,000	1.727 ms	579	< 1 µs
100,000	22.482 ms	44	< 1 µs

Table 2. *Cost of rejecting malicious status list updates*

on trust in the authority, which is expected to revoke compromised certificates accurately and in a timely manner. The exposure window discussed in the *Proposed Architecture and Practical Demonstrations* section is measured from the publication of the revocation; the delay in detecting and reporting the compromise must also be taken into account.

Given the channel being considered untrusted, an attacker may attempt the following four attack mechanisms:

- Forged list: rejected because the signature is invalid, as demonstrated in scenario S5 in the *Proposed Architecture and Practical Demonstrations* section;
- Replay of an old list: rejected since the sequence number is not greater than that of the list currently stored in the tachograph, which therefore remains in force, as demonstrated in S6 in the *Proposed Architecture and Practical Demonstrations* section;
- Flooding with forged lists: the cost of each forged list is capped by the size limit imposed by the tachograph, at approximately 22.5 ms (Table 2). Even if the attacker controls the channel, they cannot exceed its physical capacity. As demonstrated in the *Quantitative Evaluation* section, saturating the processor would require a data rate of approximately 700 Mbit/s, far exceeding the capacity of the low-bandwidth channels available to the tachograph, such as DSRC, discussed in the When Bits Attack Steel: OT/ICS Security in Transportation section;
- Blocking updates: this cannot be prevented cryptographically, and its consequences are addressed in the following paragraph.

When updates are delayed or blocked, the tachograph keeps using the stored list until its expiration date. Two behaviors are then possible. If the device continued to accept credentials after this date, a revoked card would remain accepted indefinitely, since the device would never learn of its revocation. The proposed mechanism therefore rejects all credentials once the stored list has expired (fail-closed): in scenario S7, a compromised card is accepted for at most seven days, instead of 1,757 days without the freshness check. The cost of this choice is that legitimate cards are rejected as well, so an attacker able to block updates can turn the absence of updates into a denial of service against legitimate drivers (scenario S8). The validity period of the list thus sets a trade-off between security and availability: a short period limits the use of a compromised card, but blocks legitimate cards sooner when updates are unavailable, whereas a long period tolerates longer interruptions at the cost of a longer exposure window. This period should therefore be chosen according to how often the equipment can realistically receive updates.

A relevant aspect of the proposed design is the decision to use a periodically distributed, locally verified signed list instead of an online status query. It is therefore useful to compare the proposed mechanism with established revocation approaches, namely CRLs, the Online Certificate Status Protocol (OCSP), short-lived certificates and vehicular PKIs. This qualitative comparison is based on the literature rather than on measurements.

From a structural standpoint, the proposed list most closely resembles a CRL: it is signed by the authority and contains issuance and expiration dates, as well as an increasing sequence number, fields that are also defined by the X.509 standard (Cooper et al., 2008). However, a first relevant difference lies in its compact format: the list occupies approximately 20 bytes per revoked certificate, as reported in the *Quantitative Evaluation* section, which matches the compact card-verifiable certificates of the tachograph, rather than the X.509 format. A second difference is the protection built into the mechanism: the sequence number is mandatory and prevents the reuse of an older

list (scenario S6), while the maximum list size is checked before the signature, which limits the cost of attacks (Table 2). A third difference concerns validation: the list is verified only once, upon receipt, rather than at every certificate validation, a choice that the CRL profile leaves to the implementation. Moreover, the behavior in the absence of updates is explicitly defined by the proposed mechanism: if the list has expired, credentials are rejected (scenarios S7 and S8). By contrast, measurements in the Web PKI have shown that many browsers either do not check revocation at all, particularly on mobile platforms, or accept the certificate when revocation information cannot be obtained (Liu et al., 2015).

A drawback of CRLs is that the status information may become outdated until the next update. Two alternatives have been proposed to address this issue: obtaining the status online at each validation, or making revocation unnecessary through short certificate lifetimes. In the case of OCSP, the device queries a server (the responder) at each validation as to whether the certificate has been revoked and receives a signed response in near real time (Santesson et al., 2013). This mode of operation is not suited to the tachograph, which performs validations locally, for instance when a card is inserted into the vehicle unit, without guaranteed network access. A further issue concerns privacy and availability: each query would reveal to the responder which card is used and when, and the responder becomes a single point on which validation depends; if it does not respond, the same choice described above for the Web PKI arises, namely whether to accept or reject the credential. The second alternative, short-lived certificates, makes revocation unnecessary, since a compromised certificate expires quickly (Hsu & Seymour, 1998); a dedicated extension has also been standardized to indicate that no revocation information is provided for such certificates (Housley et al., 2024). However, short-lived certificates are not suited to the tachograph either, as new certificates would have to be written into every card and vehicle unit at short intervals, which would change the personalization process and the validity periods defined for the hierarchy (Table 1).

Finally, vehicular PKIs, which also operate under intermittent connectivity, combine distributed CRLs with short-lived pseudonym certificates (European Telecommunications Standards Institute, 2022; Whyte et al., 2013). This design is driven by privacy requirements and by the very large number of credentials per vehicle, which do not apply to the tachograph, whose cards are deliberately bound to their holders. The proposed mechanism thus combines the advantages of CRLs and short-lived certificates: it operates offline, like a CRL, and bounds the exposure, like short-lived certificates, without modifying the existing certificates or hierarchy.

CONCLUSIONS

This study demonstrates that modernizing cryptographic primitives alone is insufficient to guarantee long-term cyber resilience in regulated transport infrastructure. While the European Smart Tachograph (Generation 2) successfully adopted ECC and AES algorithms, its underlying PKI maintains a static trust model. Because verification depends on offline chain validation tied to long-lived certificates, covering over 15 years for Vehicle Units and even more than 34 years for root authorities, if a credential gets compromised it can still stay accepted until it reaches its natural expiration date.

In this paper an extra credential status check layer was added on top of the existing validation mechanism, independent and lightweight, thereby closing the structural revocation gap. No changes are made to the type-approved trust anchors or to the baseline chain validation logic. The practical

demonstration showed that when revocation status is checked during local validation, the exposure window for compromised credentials shrinks substantially: from thousands of days (for example 1,757 days) down to the update interval for the status list, which runs from about 1 up to 90 days. The quantitative evaluation showed that, when the list is verified upon receipt, certificate validation remains practically as fast as in the current model (about 0.12 ms), the cost being shifted to the update (about 24 ms for 100,000 revoked certificates) and to the list size (about 2 MB). The security analysis showed that forged and replayed lists are rejected, while the validity period of the list sets a trade-off between the exposure window and the availability of legitimate cards when updates are blocked. The comparison with existing revocation mechanisms showed that the proposal is closest to a compact CRL adapted to offline validation, avoiding both the connectivity requirements of OCSP and the re-issuance cost of short-lived certificates. The evaluation has methodological limits. It was done with a functional software prototype using synthetic cryptographic material in a controlled setting, not on real physical, type-approved tachograph hardware or certified Secure Elements. Also, the attack scenarios were modeled only at the credential lifecycle level, rather than recreating the operational exploitation techniques exactly.

Future research should measure the proposed mechanism on type-approved hardware or secure elements, and investigate how revocation status lists can be efficiently distributed across existing vehicular communication channels, such as DSRC during roadside checks, periodic workshop inspection cards, and ITS-G5. Additionally, given the long operational lifecycle of root certificates, future work must examine post-quantum resilience and evaluate hybrid signature schemes suitable for memory-constrained Card-Verifiable Certificates (CVC).

REFERENCE LIST

Abudu, R., Bridgelall, R., Quayson, B. P. et al. (2025) Railroad cybersecurity: a systematic bibliometric review. *Designs*. 9(1), 23. https://doi.org/10.3390/designs9010023

Baldini, G., Sportiello, L., Chiaramello, M. et al. (2018) Regulated applications for the road transportation infrastructure: the case study of the smart tachograph in the European Union. *International Journal of Critical Infrastructure Protection*. 21, 3–21. https://doi.org/10.1016/j.ijcip.2018.02.001

Bundesamt für Sicherheit in der Informationstechnik (2021) *Common Criteria Protection Profile for Vehicle Unit (VU-PP) Smart Tachograph Gen2*. BSI-CC-PP-0094-V2-2021. Bonn, BSI. https://www.bsi.bund.de/ [Accessed 23 July 2026].

CCJ (n.d.) 'Jammers' could be a growing trend for cargo thieves. *Commercial Carrier Journal*. https://www.ccjdigital.com/business/article/14929910/jammers-could-be-a-growing-trend-for-cargo-thieves [Accessed 19 October 2026].

Chothia, T., Ordean, M., de Ruiter, J. et al. (2017) An attack against message authentication in the ERTMS train to trackside communication protocols. In: *Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security (AsiaCCS)*. Abu Dhabi, ACM, pp. 743–756. https://doi.org/10.1145/3052973.3053027

Clavijo Mesa, M. V., Patino-Rodriguez, C. E. & Guevara Carazas, F. J. (2024) Cybersecurity at sea: a literature review of cyber-attack impacts and defenses in maritime supply chains. *Information*. 15(11), 710. https://doi.org/10.3390/info15110710

Cooper, D., Santesson, S., Farrell, S. et al. (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. RFC Editor. https://doi.org/10.17487/RFC5280

Dułowicz, J., Skokowski, P. & Kelner, J. M. (2026) Experimental evaluation of GNSS receiver vulnerability to spoofing and jamming using SDR-based testbed. *Sensors*. 26(14), 4551. https://doi.org/10.3390/s26144551

European Commission (2016) Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components. *Official Journal of the European Union*. L 139, 1–503. https://eur-lex.europa.eu/eli/reg_impl/2016/799/oj [Accessed 23 July 2026].

European Commission (2021) Commission Implementing Regulation (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components. *Official Journal of the European Union*. L 273. https://eur-lex.europa.eu/eli/reg_impl/2021/1228/oj [Accessed 19 October 2026].

European Commission Joint Research Centre (2018) *Digital Tachograph System European Root Policy*. Version 2.1. JRC Technical Reports, EUR 28941 EN. https://dtc.jrc.ec.europa.eu/ [Accessed 23 July 2026].

European Commission Joint Research Centre (n.d.) *Smart Tachograph: Cryptographic Keys and Digital Certificates Sample Set*. Version 1.2. Ispra, Digital Tachograph Centre. https://dtc.jrc.ec.europa.eu/ [Accessed 23 July 2026].

European Parliament & Council of the European Union (2014) Regulation (EU) No 165/2014 of 4 February 2014 on tachographs in road transport. *Official Journal of the European Union*. L 60, 1–33. https://eur-lex.europa.eu/eli/reg/2014/165/oj [Accessed 23 July 2026].

European Root Certification Authority (2021) *ERCA Technical Specifications and Certificate Profiles for Smart Tachograph Generation 2*. Technical report. Ispra, European Commission Joint Research Centre. https://dtc.jrc.ec.europa.eu/ [Accessed 23 July 2026].

European Telecommunications Standards Institute (2022) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2. ETSI TS 102 941 V2.2.1. Sophia Antipolis, ETSI. https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf

European Union Aviation Safety Agency (2024) EASA partners with IATA to counter aviation safety threat from GNSS spoofing and jamming. Press release, 26 January 2024. https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-partners-iata-counter-aviation-safety-threat-gnss-spoofing [Accessed 19 October 2026].

Ghadge, A., Weiß, M., Caldwell, N. D. et al. (2020) Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*. 25(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Housley, R., Okubo, T. & Mandel, J. (2024) No Revocation Available for X.509 Public Key Certificates. RFC 9608. RFC Editor. https://doi.org/10.17487/RFC9608

Hsu, Y.-K. & Seymour, S. P. (1998) An intranet security framework based on short-lived certificates. IEEE Internet Computing. 2(2), 73–79. https://doi.org/10.1109/4236.670687

Inside GNSS (2017) Reports of mass GPS spoofing attack in the Black Sea strengthen calls for PNT backup. *Inside GNSS*, 24 July 2017. https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/ [Accessed 19 October 2026].

Karim, M. S. (2022) Maritime cybersecurity and the IMO legal instruments: sluggish response to an escalating threat? *Marine Policy*. 143, 105138. https://doi.org/10.1016/j.marpol.2022.105138

Kocher, P., Jaffe, J. & Jun, B. (1999) Differential power analysis. In: *Advances in Cryptology – CRYPTO '99*. Lecture Notes in Computer Science, vol. 1666. Berlin, Heidelberg, Springer, pp. 388–397. https://doi.org/10.1007/3-540-48405-1_25

Liu, Y., Tome, W., Zhang, L. et al. (2015) An end-to-end measurement of certificate revocation in the Web's PKI. In: Proceedings of the 2015 Internet Measurement Conference. ACM, pp. 183–196. https://doi.org/10.1145/2815675.2815685

Mancuso, R., Louis, A. V. & Caccamo, M. (2015) Using traffic phase shifting to improve AFDX link utilization. In: *2015 International Conference on Embedded Software (EMSOFT)*. Amsterdam, IEEE, pp. 256–265. https://doi.org/10.1109/EMSOFT.2015.7318281

Metin, B., Dümer, H. B. & Wynn, M. G. (2026) Aviation cybersecurity governance: towards an operational framework and solutions agenda for the airport domain. *Information*. 17(2), 177. https://doi.org/10.3390/info17020177

Mizrak, F. & Akkartal, G. R. (2024) Prioritizing cybersecurity initiatives in aviation: a DEMATEL-QSFS methodology. *Heliyon*. 10(15), e35487. https://doi.org/10.1016/j.heliyon.2024.e35487

National Institute of Standards and Technology (2023) *Digital Signature Standard (DSS)*. FIPS PUB 186-5. Gaithersburg, MD, NIST. https://doi.org/10.6028/NIST.FIPS.186-5

Oka, M. E., Hromada, M. & Jasek, R. (2026) Cybersecurity in critical rail infrastructure: sector specific adoption of the NIS 2 directive in Europe. *Journal of Transportation Security*. 19, 25. https://doi.org/10.1007/s12198-026-00349-8

Santesson, S., Myers, M., Ankney, R. et al. (2013) X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 6960. RFC Editor. https://doi.org/10.17487/RFC6960

Sony Semiconductor Solutions Group (2025) What is GNSS jamming and spoofing? How to detect and defend. https://www.sony-semicon.com/en/products/lsi-ic/gps/blog/20250619.html [Accessed 24 July 2026].

U.S. Maritime Administration (2017) 2017-005A-Black Sea-GPS Interference. MSCI Alert, 22 June 2017. https://cms7.marad.dot.gov/content/2017-005a-black-sea-gps-interference [Accessed 19 October 2026].

Urciuoli, L., Männistö, T., Hintsa, J. et al. (2013) Supply chain cyber security – potential threats. *Information & Security: An International Journal*. 29, 51–68.

Wachnik, R. (2025) Cyber hygiene and security training in the transport sector under the NIS2 Directive: a cross-sectoral perspective. *Communications of International Proceedings*. 2025(29), 4622825. https://doi.org/10.5171/2025.4622825

Whyte, W., Weimerskirch, A., Kumar, V. et al. (2013) A security credential management system for V2V communications. In: 2013 IEEE Vehicular Networking Conference (VNC). IEEE, pp. 1–8. https://doi.org/10.1109/VNC.2013.6737583



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.