ETSI TR 103 949 V1.1.1 (2023-05)

Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-ba3edea2b81d/etsi-tr-103-949-v1-1-1-2023-05

Reference
DTR/CYBER-QSC-0018

Keywords
ITS, migration, quantum safe cryptography

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-...
...-3ade-9b81d/etsi-tr-103-949-v1.1.1-2023-05

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-ba3cdca2b81d/etsi-tr-103-949-v1.1.1-2023-05

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document reviews the state of deployment of cryptographic security mechanisms in Intelligent Transport Systems (ITS) and Cooperative Intelligent Transport Systems (C-ITS) and their susceptibility to attack by a quantum computer. The present document makes a number of recommendations regarding the adoption of Quantum Safe Cryptography in order to minimize the exposure of ITS and C-ITS to attack.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/[illegible]-718f-4df5-a55b-ba3edea2b81d/etsi-tr-103-949-v1-1-1-2023-05

[i.1] IEEE 1609.2™: "Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages".

[i.2] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.3] FIPS 186-4: "Digital Signature Standard (DSS)".

[i.4] ANSI X9.62: "Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA)".

[i.5] FIPS 197: "Advanced Encryption Standard (AES)".

[i.6] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[i.7] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting".

[i.8] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

[i.9] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[i.10] Agreement on Technical Co-operation between ISO and CEN (Vienna Agreement).

[i.11] ISO/TS 21176: "Cooperative intelligent transport systems (C-ITS) -- Position, velocity and time functionality in the ITS station".

[i.12] ISO/TS 21177: "Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices".

[i.13] ISO/TS 21184: "Cooperative intelligent transport systems (C-ITS) -- Global transport data management (GTDM) framework".

[i.14] TS 17496: "Cooperative intelligent transport systems - Communication profiles" (produced by CEN).

[i.15] ISO/TR 21186 (all parts): "Cooperative intelligent transport systems (C-ITS) -- Guidelines on the usage of standards".

[i.16] ISO 20077-1: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 1: Content".

[i.17] ISO 20077-2: "Road vehicles -- Extended vehicle (ExVe) methodology -- Part 2: Methodology for designing the extended vehicle".

[i.18] ETSI TS 102 042 (V2.4.1): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.19] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[i.20] ETSI TS 102 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.21] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.22] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.23] ETSI GR QSC 004: "Quantum-Safe Cryptography; Quantum-Safe threat assessment".

[i.24] ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

[i.25] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.26] IETF RFC 8446: "Transport Layer Security (TLS) v1.3".

[i.27] IETF draft-tls-certieee1609-00: "Transport Layer Security (TLS) Authentication using ITS ETSI and IEEE certificates".

[i.28] ISO 20078-1: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 1: Content and definitions".

[i.29] ISO 20080: "Road vehicles - Information for remote diagnostic support -- General requirements, definitions and use cases".

[i.30] ISO 23132: "Road vehicles -- Extended Vehicle (ExVe) time critical applications -- General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)".

[i.31] ISO 20078-2: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 2: Access".

[i.32] ISO 20078-3: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 3: Security".

[i.33] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[i.34] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-ba3edea2b81d/etsi-tr-103-949-v1-1-1-2023-05

[i.35] COM(2022) 454 final: "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" (Cyber Resilience Act).

NOTE: Also available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[i.36] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

NOTE: Formerly IEEE 802.11p™.

[i.37] ETSI TS 103 759: "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2".

[i.38] ISO/TS 21185: "Intelligent transport systems -- Communication profiles for secure connections between trusted devices".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.2 Symbols

Void.

ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-ba3edea2b81d/etsi-tr-103-949-v1.1.1-2023-05

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application IDentifier
ASN.1	Abstract Syntax Notation 1
AVP	Automated Valet Parking
CA	Certification Authority
CAM	Cooperative Awareness Message
CCMS	C-ITS Security Credential Management System
C-ITS	Cooperative ITS
CPS	Certificate Practice Statement
CRQC	Cryptographically Relevant Quantum Computer
CRYSTALS	Cryptographic Suite for Algebraic Lattices
DE	Data Elements
DENM	Decentralized Environmental Notification Messages
DF	Data Frames
EA	Enrolment Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
ECTL	European Certificate Trust Lists
eIDAS	electronic IDentification, Authentication and trust Services

NOTE: As defined in Regulation (EU) 910/2014 on electronic identities and trust services (for authentication and signatures) [i.21].

ExVe	Extended Vehicle
FALCON	Fast fourier Lattice-based Compact signatures Over NTRU

FQSCS	Fully Quantum Safe Cryptographic State
G5	Variant of IEEE 802.11™ [i.36] (formerly IEEE 802.11p™) for use at 5,8 GHz and 5,9 GHz
HTTP/S	HyperText Transfer Protocol/Secure
ITS	Intelligent Transport Systems
ITS-S	ITS Station
JSON	Java Script Object Notation
MBA	MisBehaviour Authority
MBR	MisBehaviour Reporting service
NIST	National Institute of Standards and Technology
NTRU	N^{th} degree Truncated polynomial Ring Units
OBU	On-Board Unit
OBW	On Board Weighing
OBWA	OnBoard Weighing Application
PDU	Protocol Data Unit
PII	Personally Identifiable Information
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QC	Quantum Computer
QS	Quantum Safe
QSS	Quantum Safe Signature
RSU	Road Side Unit
SDO	Standards Development Organization
SLA	Service Level Agreement
SPHINCS	Stateless, Practical, Hash-based, Incredibly Nice Cryptographic Signatures
SSP	Service Specific Permissions
SVI	Secure Vehicle Interface
TLM	Trust List Manager
TLS	Transport Layer Security
TVRA	Threat Vulnerability Risk Analysis
V2V	Vehicle to Vehicle
VPN	Virtual Private Network
WAVE	Wireless Access in Vehicular Environments

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-
be3adeaf1e81/etsi-tr-103-949-v1-1-1-2023-05

4 Review of (C-)ITS architecture and security model

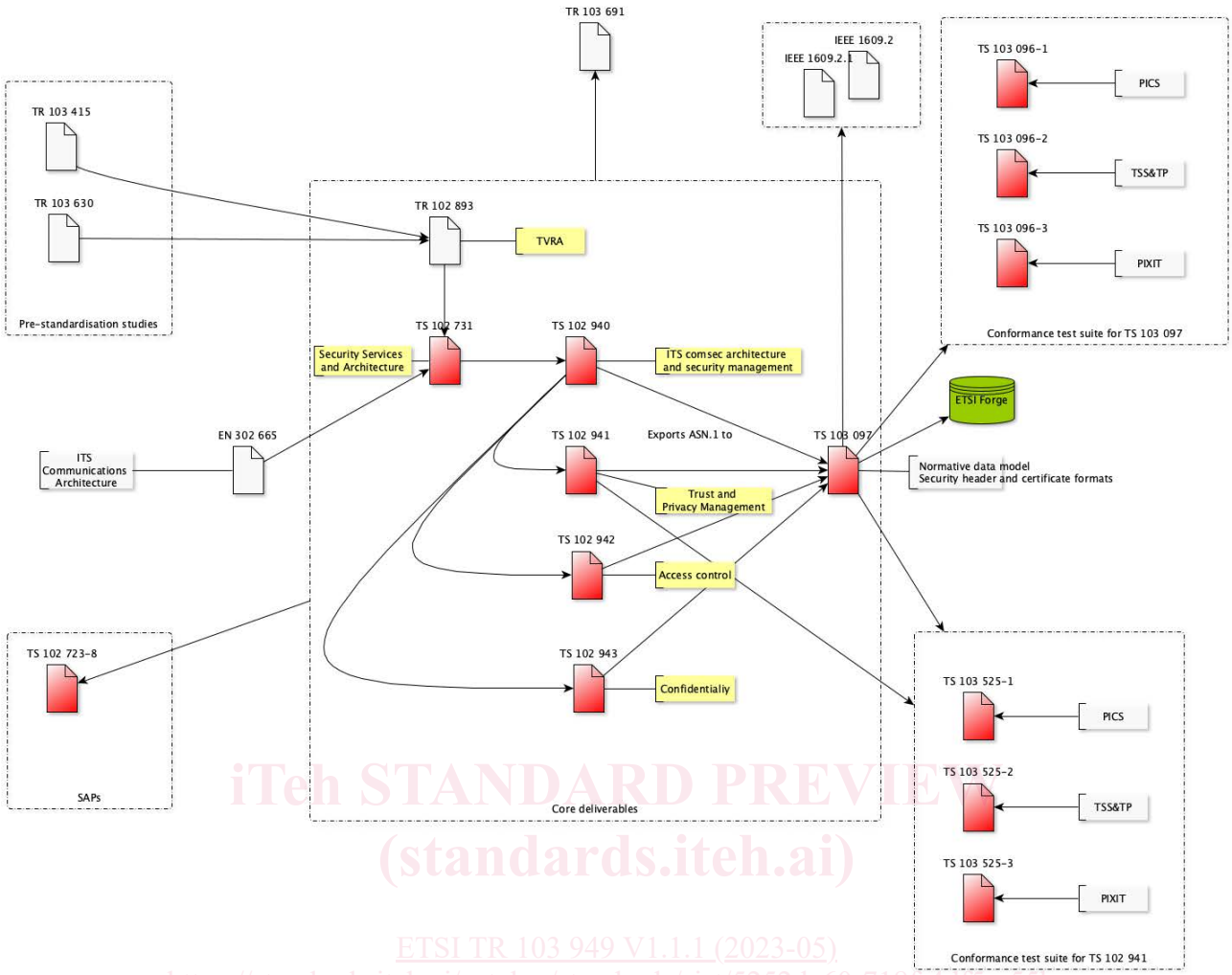
4.1 Stakeholder model

4.1.1 SDO stakeholders

The key Standards Development Organization (SDO) stakeholders in each of ITS and C-ITS are: ISO TC204; ETSI TC ITS; IEEE™ WAVE group. In addition there are several other SDO stakeholders including ETSI TC ESI (as experts in the definition and use of digital signature user the eIDAS umbrella); CEN (mirroring ISO through the Vienna agreement [i.10]), other ISO groups including ISO JTC1/SC27 WG5 addressing matters relating to privacy, IETF, NIST, ITU-T SG17 and W3C®.

In terms of the cryptographic toolkit applied in each of ITS and C-ITS the dominant parties are IEEE™ and ITU-T as developers of respectively IEEE 1609.2™ [i.1] and Recommendation ITU-T X.509 [i.2] which are the 2 public key certificate formats used in ITS and C-ITS. The primary cryptographic algorithm is the Elliptical Curve Digital Signature Algorithm (ECDSA) defined in FIPS 186-4 [i.3] and ANSI X9.62 [i.4], and where confidentiality services are applied the Advanced Encryption Standard (AES) defined in FIPS 197 [i.5] is the one that is most commonly cited.

The suite of ETSI documents that address the C-ITS security domain are shown in Figure 1.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-

Figure 1: ETSI's ITS security standards map and inter-relationships

The core requirements for authorities deploying C-ITS are also addressed in ETSI TS 102 042 [i.18].

4.1.2 Operational stakeholders

NOTE 1: This model is drawn mostly from the EU model for C-ITS and the Day-0, Day-1 safety oriented services.

Operationally in C-ITS the core components are the ITS-S (ITS Station) operated by respective stakeholders as below:

- On-Board Unit (OBU), associated to a single vehicle and likely to be associated to the vehicle owner or operator;
- Road Side Unit (RSU), associated to the road operator;
- central station, normally associated to the road operator; and
- personal unit, associated to the holder of the personal unit (it is expected that the personal ITS-S is integrated to another equipment such as a mobile phone or personal voyage unit (e.g. a bike computer)).

In addition the EU CCMS and the core ETSI Standards for C-ITS security identify two (2) forms of authority:

- Enrolment Authority (EA), the primary root authority for giving assurance of the identity of an ITS-S; and,
- Authorization Authority (AA), the independent root authority for giving assurance of the right of the ITS-S to make a claim.

The MisBehaviour Reporting service (MBR) defined in ETSI TS 103 759 [i.37] adds a MisBehaviour Authority (MBA).

Finally, for the present document, the On Board Weighing (OBW) system will add inspection authorities (standards are in development for radio based remote OBW).

In each case the operational stakeholders will need to initiate the migration process.

NOTE 2: It is anticipated that additional security requirements will be added to allow, for example, remote control of vehicles (e.g. Automated Valet Parking (AVP)), or for more nuanced vehicle types or transport users (e.g. micro-mobility solutions).

4.1.3 Supply chain stakeholders

In the ITS model there are a large number of supply chains involved. For C-ITS, and in particular for Vehicle to Vehicle safety use of C-ITS, the primary supply chain is that of the vehicle industry. Extending out from Vehicle-to-Vehicle to include Vehicle-to-Infrastructure the supply chains include that of the road operators and traffic management authorities (i.e. all roadside furniture and their back office operations). Moving beyond C-ITS and into many of the other ITS variants the supply chain includes public transport operators, city management (e.g. for smart city applications), parking operators, and the logistics domain (e.g. for just-in-time manufacturing).

A consequence of the nature of the supply chains is in the regulations that apply in placing devices on the market, many of which have very detailed requirements on security functions, on certification and similar. Thus the type approval for passenger vehicles is managed at each of national level, regional level and global level, and tends to view the vehicle as a complete entity with one centralized type approval regime. However if an ITS-S is intended to be built into a vehicle there can be a different regime for placing it on the market as part of a vehicle, from placing on the market technically similar equipment as an RSU (where different regulatory regimes apply).

4.2 Protocol and service model

iTeh STANDARD PREVIEW
(standards.iteh.ai)

For many C-ITS services, e.g. Cooperative Awareness Messages (CAM), as defined in ETSI EN 302 637-2 [i.19] there is no infrastructure.

QUOTE: "*Point-to-multipoint communication, specified in ETSI TS 102 636-3, shall be used for transmitting CAMs. The CAM shall be transmitted only from the originating ITS-S in a single hop to the receiving ITS-Ss located in the direct communication range of the originating ITS-S. A received CAM shall not be forwarded to other ITS-Ss*".

https://standards.iteh.ai/...2dc00-718f-4df5-a358-ba3edea2b81d/etsi-tr-103-949-v1-1-1-2023-05

The security model cannot be assured of having a connection to the root of trust in real time for CAM and therefore the trust model is virtualised in the certificates transmitted with each CAM (see below).

NOTE 1: The data contained in a CAM is consumed by the receiver and can be used to inform future transmissions or future behaviour of the system in which the receiver is contained.

NOTE 2: The post reception use of data from a CAM is not defined.

From a data capacity viewpoint the size of a CAM message is up to 500 bytes and a working assumption of a payload in general for ITS of about 1 kB is reasonable (the maximum limits are greater than this). As the G5 and CAM messages have only a very basic link control with no windowing or retransmission capability there is an inevitable degradation in Message Error Rate as the message size increases.

NOTE 3: The security model is predicated on a reliable transmission layer with no error propagation from lower layers.

4.3 Cryptographic model

4.3.1 C-ITS cryptographic model for CAM and DENM services

The C-ITS cryptographic model is drawn from primitives defined in IEEE 1609.2™ [i.1] and from the protocols defined in ETSI TS 102 941 [i.6]. The model for each of CAM and Decentralized Environmental Notification Messages (DENM) assumes an all-informed broadcast and data is transmitted *en-clair* accompanied by a signed attestation of authority. Each CAM and DENM transmission is composed of static vehicle data, dynamic vehicle data, and other status data.

CAM messages consist of a number of containers and the signature is calculated across the entire message. In terms of performance requirements there is a window of 50 ms defined for all processing to be completed across a hop, and the repetition rate of CAM is up to 10 Hz, thus about 100 ms between transmissions. In the scope of CAM and C-ITS as a safety multiplier it has to operate in near real time thus making the transmission latency introduced by source/destination processing ideally closer to zero than the 50 ms allowed. In common with all ECDSA signature schemes there is a new random element required in every signature to minimize exposure of the secret key.

In general C-ITS messages are signed using a pseudonymous attribute or authorization key. There is no conventional session based communications architecture in C-ITS, although this does not hold true for all ITS services. As there is no online verification available, public key certificates are distributed alongside messages. Not all messages are mandated to carry the Public Key Certificate (PKC) but without doing so, and without either online access to a PKC repository or a reverse channel to request the PKC, there is a risk of being unable to verify the message.

4.3.2 Core C-ITS message structures

4.3.2.1 CAM structure

For vehicle ITS-Ss the CAM comprises one basic container and one high frequency container, and can also include one low frequency container and one or more other special containers (see Figure 2):

- the basic container includes basic information related to the originating ITS-S;
- the high frequency container contains highly dynamic information of the originating ITS-S;
- the low frequency container contains static and not highly dynamic information of the originating ITS-S; and
- the special vehicle container contains information specific to the vehicle role of the originating vehicle's ITS-S.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TR 103 949 V1.1.1 (2023-05)
https://standards.iteh.ai/catalog/standards/sist/5252de60-718f-4df5-a55b-ba3edea2b81d/etsi-tr-103-949-v1-1-1-2023-05