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

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

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

Contents

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.

Foreword

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

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.

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.

[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).

[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.

3.2 Symbols

Void.

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

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.

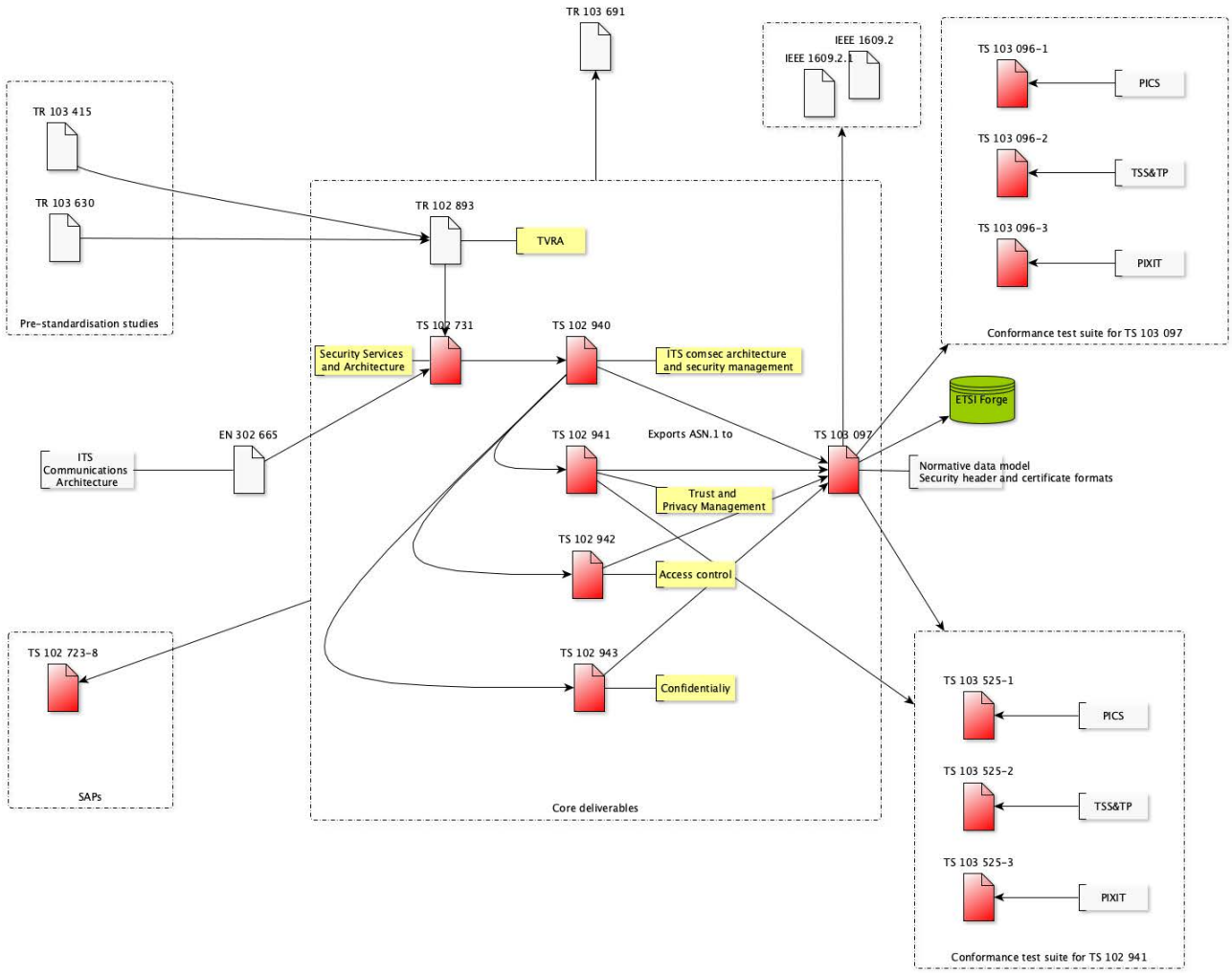

Figure 1: ETSI's ITS security standards map and inter-relationships

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

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*".

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.

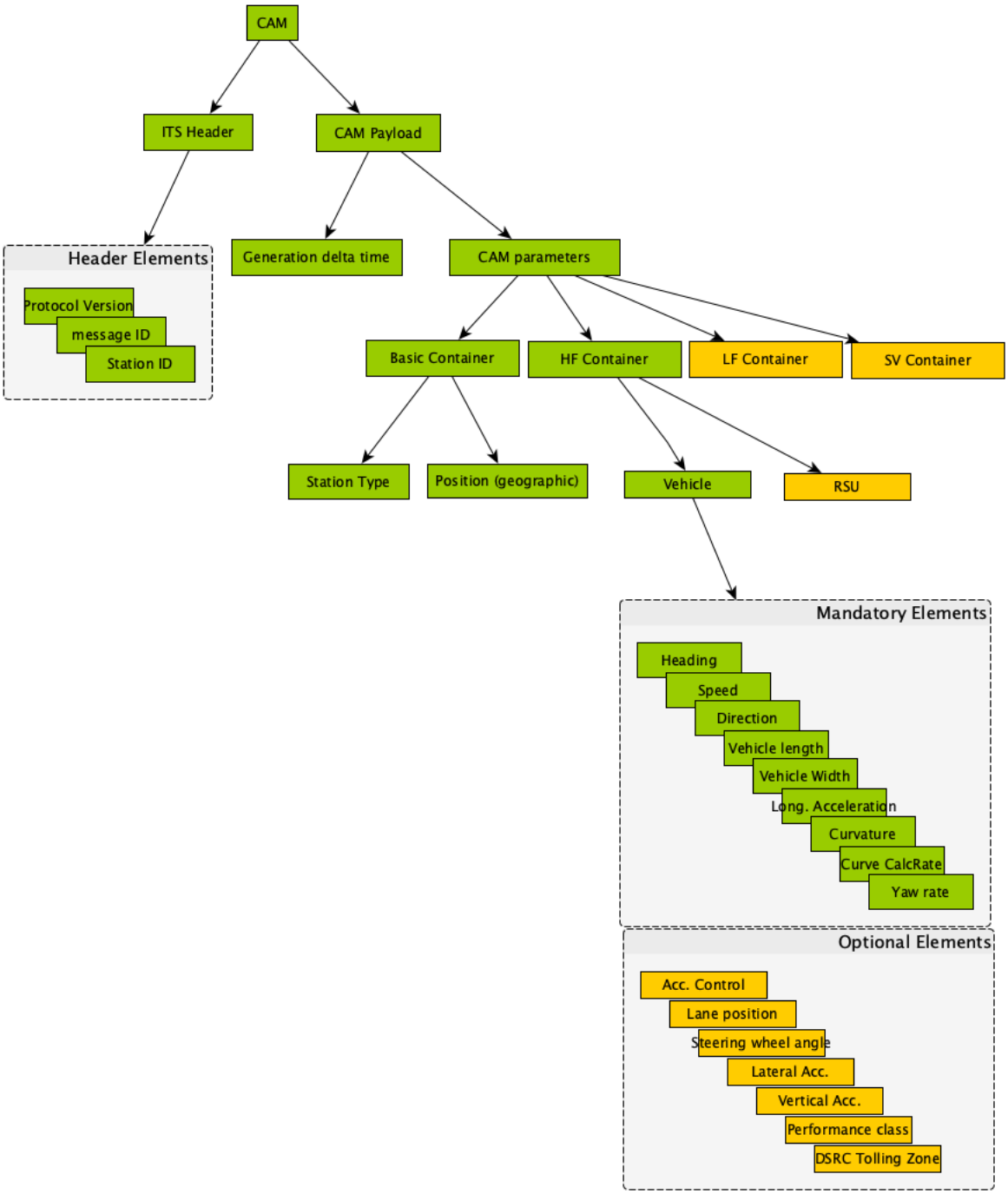

Figure 2: ETSI CAM message structure, example for vehicular CAM

All CAMs generated by a RSU ITS-S have a basic container and optionally more containers.

4.3.2.2 DENM structure

A DENM is composed of a common ITS Protocol Data Unit (PDU) header and multiple containers, which constitutes the DENM payload:

- The ITS PDU header is a common header that includes the information of the protocol version, the message type and the ITS-S ID of the originating ITS-S.

- The DENM payload consists of four (4) fixed order parts: the management container, the situation container, the location container and the à la carte container:
  - The management container contains information related to the DENM management and the DENM protocol.
  - The situation container contains information related to the type of the detected event.
  - The location container contains information of the event location, and the location referencing scheme (i.e. the coordinate scheme used for the location data).
  - The à la carte container contains information specific to the use case which requires the transmission of additional information that is not included in the three (3) previous containers.

For all types of DENM, the ITS PDU header and the management container are always present. The situation container, the location container and the à la carte container are optional containers. For a cancellation DENM or a negation DENM, the situation container, location container and à la carte container are not present. If the situation container is present, the location container will be present as well. The à la carte container is present only when applicable as specified in application specification standards.

The general structure of a DENM is illustrated in Figure 3. Each container is composed of a sequence of Data Elements (DE) and/or Data Frames (DF). A DE and a DF is either optional or mandatory.

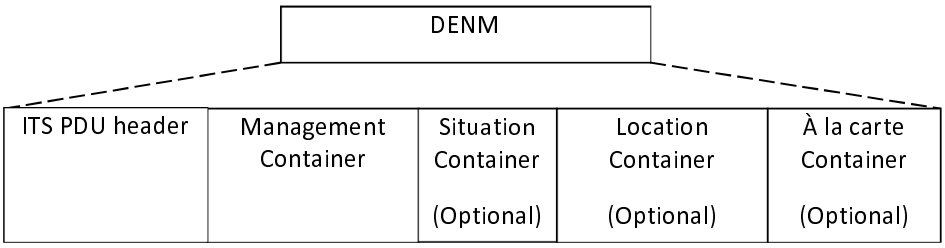

Figure 3: General structure of a DENM (Source: ETSI TS 102 637-3 [i.20])

4.3.3 C-ITS signature using IEEE 1609.2 certificate structure

In ETSI EN 302 637-2 [i.19] the security constraints are described in a signed object. In addition the root structure of the signature is common across global regions with some very minor terminology variations. Therefore the discussion below applies across all geo-regions unless indicated otherwise.

The security mechanisms for ITS consider the authentication of messages transferred between ITS-Ss with certificates. A certificate indicates its holder's permissions to send a certain set of messages and optionally privileges for specific data elements within those messages. The format for the certificates is specified in ETSI TS 103 097 [i.9].

Within the certificate the permissions and privileges are indicated by a pair of identifiers, the ITS-AID and the SSP:

- The ITS-Application Identifier (ITS-AID) as defined in ETSI TS 102 965 [i.33] indicates the overall type of permissions being granted.

EXAMPLE 1: There is an ITS-AID that indicates that the sender is entitled to send CAMs.

- The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID.

EXAMPLE 2: There can be an SSP value associated with the ITS-AID for CAM that indicates that the sender is entitled to send CAMs for a specific vehicle role.

An incoming signed CAM is accepted by the receiver if the certificate is valid and the CAM is consistent with the ITS-AID and SSP in its certificate. AIDs and SSPs are hierarchical and an SSP only has meaning for an AID.

4.3.4 Authorization model for vehicular data access

There are two core models for giving 3rd party access to vehicular data:

- ExVe (defined in ISO 20077-1 [i.16] and ISO 20077-2 [i.17]) makes a secured connection from the vehicle to an off-site data centre with all data transmissions protected by a VPN connection. Access to the off-site data centre is not specified but is assumed to be available using conventional cloud data access models (e.g. using a combination of JSON and HTTP/S).
- SVI is a suite of standards to enable on-vehicle access to data from an external 3rd party. The core model of SVI is that of cryptographically assisted access control to identified parties. The underlying identity and attribute assertion model used is based on both Recommendation ITU-T X.509 [i.2] and IEEE 1609.2 [i.1] certificates with ECDSA signatures.

4.4 Summary of Quantum Computing threat to ITS

Notwithstanding the overall summary of the scope of ITS and C-ITS as described above, the immediate concern is with the risk to ITS and C-ITS as a whole by the existence of a Cryptographically Relevant Quantum Computer (CRQC). The overall threat from Quantum Computing on the security of ICT networks as described in ETSI EG 203 310 [i.22] and in ETSI GR QSC 004 [i.23] is critical. In using current elliptical curve cryptography there is a substantial risk of masquerade (impersonation attack) and that can lead to collapse of the required trust model.

Applying the risk model from ETSI TS 102 165-1 [i.25] has uncertainty only on the timetable for when a QC will exist but once it exists the impact will be High, and the likelihood of an attack similarly considered as Likely, leading to critical risk (see Table 1).

Table 1: Risk assessment for the application of a CRQC to ITS/C-ITS keying infrastructure

Point of attack	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
				Factor	Analyst estimation	Value	Potential	Likelihood		
Keying infrastrucure	Availability	Manipulation	Application of a quantum computer to the keying infrastructure of ITS/C-ITS. It is assumed for this that readily available and understood attacks using a public key certificate as the input to recover the matching private key are enabled. The metrics in the assessment are based on the assumption that a valid QC exists	Time	<= 1 day	0	Basic	Likely	High	**Critical**
				Expertise	Layman	0				
				Knowledge	Public	0				
				Opportunity	Unnecessary	0				
				Equipment	Standard	0				
				Attacker Theat level		Low				
				Attacker motivation	Low (curious)					
				Attacker capability	Limited					
				Asset Impact	High	3				
				Resultant impact	High	3				
				Intensity	Single instance	0				

NOTE: The assessment of factors for the attack makes an assumption that Quantum Computing resources will be widely available using web-services with most development environments also making APIs available to access such resources hence the rating of "Standard" for equipment. In addition the time taken to develop and launch an attack is assessed to be very low as there is a lot of already published knowledge of how to use QCs in attacks to recover private keys.

The analysis is independent of the specific nature of any ITS/C-ITS solution as the loss of trust in the entire suite of ITS models is what is critical.

The timeliness of addressing the risk is discussed in ETSI GR QSC 004 [i.23]. The risk is critical as seen above. The equation given in [i.23] is simple:

- X = the number of years the public-key cryptography needs to remain unbroken.
- Y = the number of years it will take to replace the current system with one that is quantum-safe.
- Z = the number of years it will take to break the current tools, using quantum computers or other means.
- T = the number of years it will take to develop trust in quantum safe algorithms.

If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. The X factor has to consider the lifetime of devices in the field, which for vehicles (OBUs) and for some infrastructure (RSUs) is likely to be significant (20 years say). The Y factor is very dependent on the nature of the cryptographic deployment but the present document is a part of the assessment of Y.

5 Application of ETSI TR 103 619 to C-ITS

5.1 Overview

In simple terms the stages in migration to a Fully Quantum Safe Cryptographic State (FQSCS) outlined in the present document, building on the core framework of migration defined in ETSI TR 103 619 [i.24], is a specific mitigation to the general threat from quantum computing that is outlined in the ITS TVRA found in ETSI TR 102 893 [i.7].

NOTE: The ITS TVRA in ETSI TR 102 893 [i.7] is being updated to adopt the latest framework from ETSI TS 102 165-1 [i.25] and only when that exercise is complete will the QC threat to ITS be fully documented.

As ECDSA is considered to be vulnerable to quantum computer-aided attacks the risk of invalidating the entire trust architecture of C-ITS is assessed as critical (see Table 1 in clause 4.4). The overall complexity of the key management scheme is a further significant threat (see Annex A for details of the EU's scheme for deployment of ITS).

5.2 Stage 1 - Inventory compilation

The simplest way to compile an inventory of the at-risk C-ITS assets is to add any device acting as an ITS-S to the inventory. The following variants of an ITS-S are described:

- ITS-S Vehicular mount (On-Board Unit (OBU));
- ITS-S for roadside use (Road Side Unit (RSU));
- ITS-S personal station (e.g. integrated to a personal mobile device such as a mobile phone, bike computer); and
- ITS-S central station (e.g. integrated as part of a back-office facility in traffic management).

In addition to the stations themselves are the authorities defined for the trust management framework:

- Enrolment Authority (EA);
- Authorization Authority (AA);
- MisBehaviour Authority (MBA); and
- OnBoard Weighing inspection Authority (OBWA).

As noted in ETSI TR 103 619 [i.24] the assumption is that migration is "like for like", i.e. that an asymmetric cryptographically protected asset will be protected in like manner after migration, and that symmetric cryptographically protected assets will likewise also be protected in like manner after migration. However it is also core to the migration that such a like for like approach does not ignore a review of strategy. A key requirement of migration is therefore to verify if design decisions made for the pre-QSC era are still valid for the QSC era. The working assumption is that a like-for-like migration is to be undertaken, replacing asymmetric cryptography with asymmetric cryptography, however that assumption should be verified. Tables 2, 3, 4, 5 and 6 address the sample questions from ETSI TR 103 619 [i.24] for the C-ITS model defined by ETSI's ITS group with respect to the standards environment.

NOTE: A vendor, operator or other stakeholder in answering these questions can arrive at different conclusions than those from a standards development perspective.

Table 2: Risk assessment questions

Magnitude	What risks will information disclosure create? Classifications of where risk lies include: Monetary loss (i.e. direct financial impact), Compliance (i.e. will existing compliance procedures be maintained?), Legal (e.g. will existing legal safeguards apply?), Reputation (e.g. how will readiness or failure be ready to impact the reputation of the organization either in absolute terms or by comparison to peer and competitor organizations?).	As CAMs and DENMs are sent in clear there is no risk of information disclosure. The risk is that the trust network is broken. The ability to maintain privacy can be lost with a risk that the functionality of C-ITS will be disabled in order to prioritize user privacy.
Duration	How long has confidentiality to be maintained for each asset or class of assets?	Privacy of the user is to be maintained across the lifetime of the ITS-S that is associated to the user.
Scope	Are keys or certificates issued by the affected organization to third parties? Under what Certificate Practice Statement (CPS) or Service Level Agreement (SLA)?	In conventional ITS-S it can be classified as all parties being 3rd parties. The EA manages many of the roles of AAs but AAs have no commercial or organizational relationship to the EA, nor to the ITS-Ss that they authorize. There is no explicit SLA in C-ITS although the policy management structure, and the role of the EA and AA in distribution of certificates, will maintain a form of SLA that is then implicit in the overall system structure.
Duration	Can damage due to degradation or interruption of each service that uses crypto be quantified?	No. The system is designed as a safety multiplier in the first instance.
Response	Is there a plan to protect encrypted assets in case of a crypto failure?	N/A

Table 3: Data assessment questions

Type	What classes of data are subject to encryption? (PII, Trade Secret, Custodial Secret, Government Classified, etc.)?	Primarily PII in the context of C-ITS achieved by use of pseudonymous keying and signed transfer of attributes related to the ITS-S rather than by encryption.
Protection duration	How long does confidentiality need to be maintained for each data class?	N/A
Retention	Is encrypted data deleted according to a regular schedule?	N/A
Disclosure impact	What are the consequences of disclosure of each data class?	None per se. There is a risk of exposure of behaviour but that is also the purpose of C-ITS, i.e. that the current dynamics of an ITS-S are exposed within a trusted environment.
Exposure	Is encrypted data normally exposed to potential attackers? (e.g. in transit or public cloud)?	N/A

Table 4: Cryptographic assessment questions

Type	For each key, what is the strength, the algorithm binding, and the usage (signature or encryption, application specific security, etc.)?	ECDSA with Brainpool and NIST curves. Keys are bound to attributes (for AA tickets) or to a canonical identifier (for EA tickets).
Strength	What is the effective strength of each key in view of classical and quantum attacks?	Equivalent to 128 bit classical security.
Lifetime	What are the issuance and expiration dates for each key?	The Enrolment key is long lifetime key (expiry times of (say) 25 years). AA ticket keys are short life, expiry times of (say) a few months.
Management	Are all keys inventoried and locatable? Are keys easy to revoke and reissue?	AA keys are difficult to revoke and are not intended to be reissued. EA tickets are not intended to be re-issued but can be revoked and replaced.

Table 5: Infrastructure inventory questions

Crypto software inventory	What crypto libraries are in use? What protocol libraries are in use?	N/A from a standards viewpoint.
Key inventory	What keys are in use, by what applications?	N/A from a standards viewpoint.
Admin inventory	Who (or what role) is authorized to manage which keys and which crypto modules and devices?	This is addressed in the policy for C-ITS.
Certificate inventory	What certificates are issued to the organization? Who issued them?	The EA and AA in common with normal practice should maintain an audit control of all certificates they have issued and to whom. The concern is that the AA will issue 100 s of certificates per ITS-S over its lifetime and that there will be many million ITS-Ss at any one time. In the event of a quantum computer aided attack (i.e. the presence of a cryptographically relevant QC) all issued certificates will be at risk and all will need to be updated.
Crypto hardware inventory	What crypto hardware is in use? What attributes does each certificate have?	N/A from a standards viewpoint.
Application inventory	Which applications use which libraries, which keys, and which protocols?	N/A from a standards viewpoint.

Table 6: Supplier inventory questions

Certification Authorities (CAs)	Do the organization's CA agreements hold the CA to an SLA for timely reissuance? Does the organization backup CA under contract?	N/A from a standards viewpoint
Code signatures	Can and will application vendors in the supply chain re-sign applications in a timely way?	N/A from a standards viewpoint
Service Level Agreements (SLAs) with the CA	Do revocation and reissuance requests get priority vs. other firms in emergencies?	N/A from a standards viewpoint
SLAs with the data custodian	What obligations do the custodians of data have in case of algorithm breach?	N/A from a standards viewpoint
CSRs	Does the organization retain CSRs in order that the organization can request reissuance of certs with the correct attributes?	N/A from a standards viewpoint
SLAs with software vendors	Are vendors in the supply chain obligated to timely upgrades to fix crypto breaches? (see note)	N/A from a standards viewpoint
NOTE: This is likely to be a specific requirement if the vendor is subject to the constraints of the EU Cyber Security Act [i.34] or the EU Cyber Resilience Act [i.35].		

5.3 Stage 2 - Preparation of the migration plan

5.3.1 Overview of process

As outlined in ETSI TR 103 619 [i.24] the migration plan should include the following:

- A full inventory of assets.
- For each asset:
  - Whether a given asset will be migrated.
  - When a given asset will be migrated.
  - An orderly sequence of migration of inter-dependent assets.
  - The migration solution chosen for each given asset: replacement by full QS crypto or a hybrid solution.

- Testing including dependency testing.

The present document addresses the inventory only in general terms by identifying the ITS-S as the "at risk" element.

In the outline threat assessment given in clause 4.4 and in Table 1, the conclusion is that a quantum computing attack on C-ITS results in a critical risk to the system, it can also be suggested that this is an existential level threat as it removes the trust from the roots of trust in the system. To re-assert trust every asset used in the trust model needs to be migrated to a quantum safe state.

Given the number of affected devices and the risk factors outlined in clause 4.4 it is suggested that a hybrid mode is not adopted subject to more detailed analysis. The immediate concern is that hybridization may adversely impact the X factor (see clause 4.4). The existing standards in ITS recommend a degree of crypto-agility and given that the current signature modes rely on conventional cryptographic hashing algorithms it is recognized that some QS algorithms, based on hashing, can be deployed relatively quickly (see clause 5.3.2 for a more detailed discussion).

5.3.2 Algorithm selection and protocol definition

The intent is to migrate from the ECDSA algorithm and its associated keys to an equivalent strength quantum safe algorithm. The NIST list of algorithms in Table 7 have been identified as believed to be quantum safe.

NOTE 1: There is a wide set of views of what security strength means, for the present document the assumption made is that ECDSA P-256 provides 128-bit classical security strength and is equivalent to an RSA 3 072 key.

NOTE 2: Table 7 identifies parameter and signature size against NIST security level 5.

Table 7: NIST list of quantum safe signature algorithms candidates to be standardized

Algorithm	Outline	Signature size (L5)	Key sizes (L5)	Suitability to ITS
CRYSTALS-Dilithium (Cryptographic Suite for Algebraic Lattices)	Recommended by NIST as a primary algorithm.	4 595 bytes	Public 2 592 bytes Private 4 864 bytes	No. The signature size is significantly in excess of the payload capacity of the G5 radio link.
FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU)	Noted by NIST for applications where a smaller signature is required. NIST has noted that implementation is "difficult" and side channel protection is required. In particular floating point arithmetic units are required for implementation.	1 280 bytes	Public 1 793 bytes Private 13 953 bytes	Marginal as the signature size is at the absolute limit of G5 capacity.
SPHINCS+ (256 s) (read as "Sphincs plus") (Stateless, practical, hash-based, incredibly nice cryptographic signatures)	Noted by NIST as a backup as the mathematical basis is different from the others. SPHINCS+ is based on conventional hash algorithms (SHA256) but in a very complex set of structures.	29 792 bytes	Public 64 bytes Private 128 bytes	No. The signature size is significantly in excess of the payload capacity of the G5 radio link.

As Table 7 makes clear the Quantum Safe Signature algorithms identified by NIST for standardization yield signatures that exceed the capacity of the radio channel of C-ITS. Whilst this is not of itself insurmountable it does suggest that by signing every transaction, which is necessary to ensure trust in the system, that security data (the signature, certificates, keys) will dominate and perhaps overwhelm the system function.

It is not the purpose of the present document to suggest specific algorithms, however it is recognized that NIST has stated that it will standardize quantum safe signature algorithms as listed above. It is further acknowledged that this is not the final set of algorithms that NIST will publish, rather NIST will continue to consider new algorithms. It should however be acknowledged that there is no significant advantage in waiting for an ideal algorithm to be developed as that severely impacts on the time factors outlined in ETSI GR QSC 004 [i.23] thus potentially increasing the risk to the system (even though it is already assessed as critical any additional delay only reinforces the criticality of the threat).

A concern from the current C-ITS architecture is that the public keys required for verification are not pre-installed at the receiving unit. Therefore in addition to the signature it is essential to also build in capacity to exchange the public key. Hence the combined size of the signature and the public key needs to be considered, as does the fact that the public key is signed (and attested to) by a 3rd party. The certificate is not required to be attached to every transaction, but it is still the case that for many transactions, 2 (two) signatures (one on the message, and one on the key) and the public key are sent. Table 8 gives estimates of the capacity required for such a transmission, excluding the payload itself.

Table 8: Estimated capacity required in C-ITS messages

Algorithm	Estimated capacity required in C-ITS messages
CRYSTALS-Dilithium	11 782 bytes
FALCON	4 353 bytes
SPHINCS+ (256 s)	59 648 bytes

5.4 Stage 3 - Migration execution

5.4.1 Trust management during migration

Stage 1 will identify the trust infrastructures (see also Annex C). During stage 2 a determination is made of the degree of continuity of the trust infrastructures (e.g. the roles and relationships in the trust infrastructure, and the associated key management infrastructure).

EXAMPLE: A Root CA can require that verification of CA keys is done in a face-to-face signing ceremony and thus the scheduling of such ceremonies as well as the distribution of new keys and certificates throughout the infrastructure will need to be considered in the planning of migration.

A number of functions can be reliant on specific roots of trust and the transfer of each root of trust to a Quantum Safe model is a key element that is present in the migration plan.

5.4.2 Isolation approaches during migration

In a conventional system it is suggested in ETSI TR 103 619 [i.24] that not all systems will be updated at the same time. This is probably not a straightforward approach in C-ITS where vehicles are isolated from the system for long periods of time, and where vehicles are unconstrained in movement across national and trust boundaries.

Annex A: Migration guidance for QSC provisions in ETSI ITS standards

The ETSI ITS standards are at the root of the European Union C-ITS Security Credential Management System (EU CCMS) which includes a number of certificate and signature forms, including:

- Trust List Manager (TLM) certificates
- European Certificate Trust Lists (ECTL)

The primary certificate type in ETSI is the ASN.1 data type `EtsiTs103097Certificate` which is defined as follows (all certs in C-ITS are of the same format):

```
EtsiTs103097Certificate::= Certificate (WITH COMPONENTS{...,
  toBeSigned (WITH COMPONENTS{...,
    id (WITH COMPONENTS{...,
      linkageData ABSENT,
      binaryId ABSENT
    }),
    certRequestPermissions ABSENT,
    canRequestRollover ABSENT
  })
})
```

Where `Certificate` comes from IEEE 1609.2 [i.1] (see also Annex B) as follows:

```
Certificate ::= CertificateBase (ImplicitCertificate | ExplicitCertificate)

SequenceOfCertificate ::= SEQUENCE OF Certificate

CertificateBase ::= SEQUENCE  {
    version                 Uint8(3),
    type                    CertificateType,
    issuer                  IssuerIdentifier,
    toBeSigned              ToBeSignedCertificate,
    signature               Signature OPTIONAL
}
```

The `Signature` field in the `Certificate` is marked as Optional in order not to enforce its transmission and thus cut the bandwidth of exchanges (explicit certs have the signature, implicit certs do not). For C-ITS transmissions, only ECDSA signatures are allowed with one of 3 curves allowed (NIST-P256, Brainpool-P256, Brainpool-P384).

```
Signature ::= CHOICE  {
    ecdsaNistP256Signature        EcdsaP256Signature,
    ecdsaBrainpoolP256r1Signature EcdsaP256Signature,
    ...,
    ecdsaBrainpoolP384r1Signature EcdsaP384Signature
}

EcdsaP256Signature ::= SEQUENCE  {
    rSig     EccP256CurvePoint,
    sSig     OCTET STRING (SIZE (32))
}

EcdsaP384Signature ::= SEQUENCE  {
    rSig     EccP384CurvePoint,
    sSig     OCTET STRING (SIZE (48))
}
```

As seen above the signature fields are 32 or 48 bytes (i.e. 256 or 384 bits) with the curve point of the same size, resulting in a minimum signature size of 64 or 96 bytes (the actual transmitted size is dependent on the encoding scheme).

Whilst technically adding a Quantum Safe algorithm would appear to be a case of extending the `Signature CHOICE` to include new algorithms this, however, is not the primary problem as this would not account for the increase in bandwidth required to process and transfer signed data.

It is also recognized that the IEEE 1609.2 [i.1] development group (see also Annex B) has developed guidance for adding algorithms to IEEE 1609.2 [i.1] (not reflected in the publicly available specification at the time of writing).

Annex B:
Migration guidance for QSC provisions in IEEE 1609.2 and associated standards

The same argument applies to IEEE 1609.2 [i.1] as applies to the QSC provisions in ETSI ITS standards in Annex A.

Annex C:
Migration guidance specific to EU CCMS model

The EU C-ITS Security Credential Management System (EU CCMS) has been developed in order to enable the deployment of the EU's C-ITS framework under the C-Roads pilot system. The model is bolstered by a number of policy framework documents in addition to the core PKI model, which is broadly defined to support the security architecture from ETSI TS 102 731 [i.8] and in the protocol documents ETSI TS 102 941 [i.6] and respecting the data models given in ETSI TS 103 097 [i.9] and using the framework of IEEE 1609.2 [i.1] certificate services.

It is recognized that EA Certs have been extended to allow the use of X.509 signatures and infrastructures.

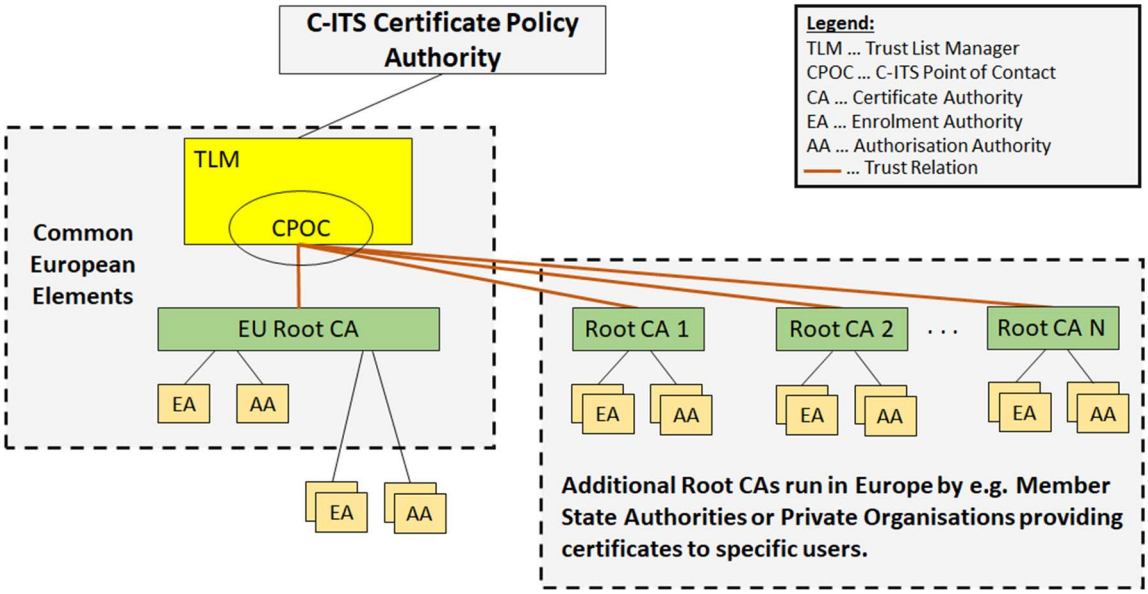

Figure C.1: EU CCMS basic model

The major deviations of the EU's CCMS to the simple model of ETSI TS 102 731 [i.8] is in the addition of a Trust List Manager (TLM) to coordinate the various root CAs.

As an example of a hierarchy a full switchover to the FQSCS requires that when the Root-CA changes to a new quantum safe crypto model that all other entities have the ability to switch. In such a system it is recommended that the rollout of quantum safe crypto capabilities begin at the bottom of the hierarchy and are confirmed prior to switchover.

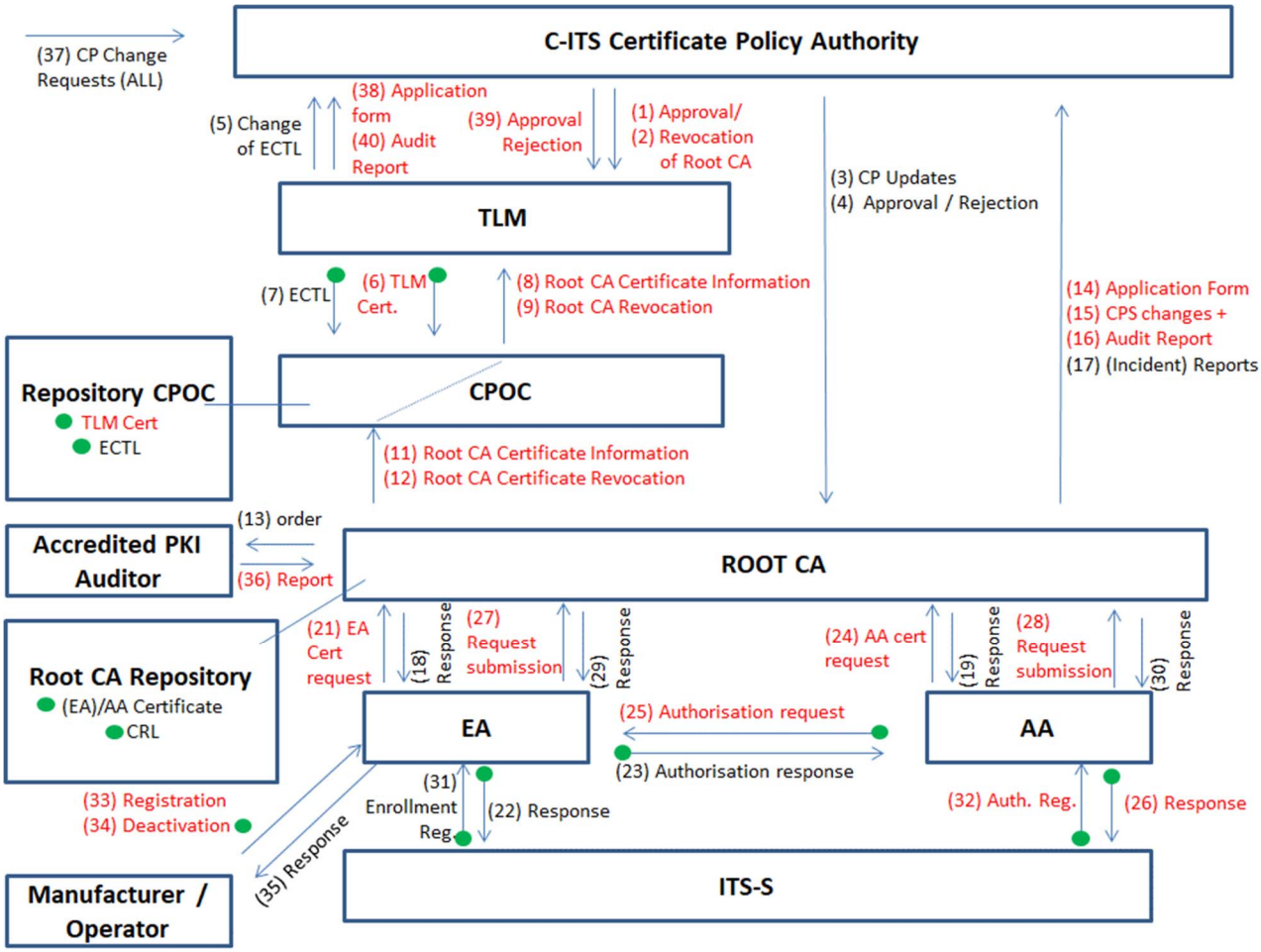

Figure C.2: EU CCMS message flows (example)

Annex D:
Migration guidance specific to SVI model

The Secure Vehicle Interface (SVI) is an umbrella term used to describe a set of ISO and CEN standards that address a range of use-cases for connected vehicles in an intelligent transportation system where there is a requirement for access to vehicle telematics directly from the vehicle. These standards include:

- ISO/TS 21176 [i.11] addressing position, time and velocity of a vehicle.
- ISO/TS 21177 [i.12] addressing the source, authenticity and integrity of data exchanged between entities, for example a vehicle and a trusted device or server.
- ISO/TS 21184 [i.13] addressing the configuration of data sets and data elements.
- TS 17496 [i.14] and the almost identical ISO/TS 21185 [i.38] addressing communication protocols.
- ISO/TR 21186 [i.15] provides guidelines for usage of standards within the context of intelligent transportation systems.

As is shown in Figure 9 titled "Interactions between local functional elements" in ISO/TS 21177 [i.12], the security protocol mechanism is anticipated to use Transport Layer Security (TLS) v1.3 specified in IETF RFC 8446 [i.26] with the amendment defined in Internet Engineering Task Force Draft, Transport Layer Security (TLS) Authentication using ITS ETSI and IEEE™ certificates [i.27] to permit IEEE 1609.2 [i.1] certificates.

The security model of ISO/TS 21177 [i.12] is intended to offer source authenticity, proof of the integrity of data exchanged, and can also provide confidentiality protection of the data exchanged. The impact on ISO/TS 21177 [i.12] is the same as that for any other application building on TLS with IEEE 1609.2 [i.1] (or in fact any scheme built on vulnerable cryptographic models).

Annex E:
Migration guidance specific to ExVe model

The extended vehicle data model allows a manufacturer to take telematics data from a vehicle and make it available to 3rd parties from an off-vehicle data server. The link from vehicle to off-vehicle data store is enabled using a VPN connection, whilst the link of 3rd party to the data store is likely also to be via a VPN this is subject to the Vehicle Manufacturer.

Several ISO standards defining the Extended Vehicle have either been adopted or are being finalized:

- ISO 20077 defines the general framework for the Extended Vehicle:
  - ISO 20077-1 [i.16] defines the concepts and terms for the Extended Vehicle;
  - ISO 20077-2 [i.17] specifies the methodology for designing the extended vehicle (security, safety).
- Two complementary standards provide for the use of the Extended Vehicle for over-the-air services:
  - ISO 20078-1 [i.28], ISO 20078-2 [i.31] and ISO 20078-2 [i.32] provide the framework for the use of web services;
  - ISO 20080 [i.29] defines a first use case: Remote diagnostic support.
- ISO 23132 [i.30] addresses the peri-vehicular communication of time constrained data relating to road safety (e.g. V2V).

Many of the details of the security model of ExVe are not fully defined by the standard but, rather, uses conventional web-services models including the associated models in TLS, HTTP/S and so forth. In approximate summary the model of ExVe as stated requires that each vehicle creates a VPN connection to a manufacturer designated host.

The ExVe assets can be assumed to be in the control of a single entity thus there is a lower risk to the success of the migration as fewer entities are involved.

Every vehicle in the ExVe domain will require to be updated with support for the selected QSC algorithm. Each unique key pair in the system will require to be updated as appropriate to the new algorithm and the key certificate chain will need to be rebuilt (from top down).

Annex F:
Very simple overview of ITS and C-ITS

Intelligent Transport Systems (ITS) address a massive range of technologies that between them enable more efficient transport of people and goods. ITS is by default multi-modal, in other words it addresses every form of transport from pedestrian travel, through human powered vehicles, to all forms of powered vehicles, thus including road vehicles, off-road vehicles, industrial vehicles, rail vehicles (including light rail, underground services, trams and conventional heavy rail) and so forth. In addition ITS has multiple intentions, including logistics management (moving goods and people efficiently).

The Cooperative ITS sub-domain has been designed to act as a safety multiplier by exchanging dynamic vehicle data in a local area.

The impact of a Quantum Computer to C-ITS before C-ITS has migrated to a Quantum Safe Cryptographic platform is an existential level event. If trust in the system is lost, any data in the system, and the entities that rely on that data, will be unable to distinguish valid from invalid data, and valid from invalid entities. The recommendations made in the present document therefore fall into two threads:

1) To drive migration from the policy for C-ITS.

2) To review the overall security architecture in C-ITS and its application to a more general ITS model.

The current security architecture of C-ITS is based on a split authority model, and more fundamentally in the attestation and verification of authorization to make certain claims.

Annex G: Bibliography

- ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".
- ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access Control; Release 2".
- ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services; Release 2".
- ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

History

Document history		
V1.1.1	May 2023	Publication