ETSI TR 103 971-1 V2.1.1 (2026-05)

TECHNICAL REPORT

Intelligent Transport Systems (ITS);
Security;
Feature specific Threat, Vulnerability and Risk Analysis (TVRA);
Part 1: Infield Test mode, Quantum safety;
Release 2

Reference
DTR/ITS-00546

Keywords
authentication, authorization, confidentiality, security

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Intelligent Transport Systems (ITS).

The present document is part 1 of a multi-part deliverable, each part containing one of more specific application notes documenting the TVRA results for a specific application.

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 summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of a number of aspects of an Intelligent Transport System (ITS) by means of application notes. Each application note is addressed in a distinct sub-part and considers the threat to existing and planned vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.2] operating in a fully deployed ITS.

The present document extends but does not replace previous publications addressing TVRA in ITS, e.g. in ETSI TR 102 893 [i.16].

NOTE: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the ETSI ITS Work Programme.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

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

[i.2] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Release 2".

[i.3] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.4] ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

[i.5] ETSI TR 103 949: "Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study".

[i.6] ETSI TS 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".

[i.7] ETSI TS 103 300-2: "Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2".

[i.8] CCMB-2022-11-001: "Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model", November 2022, Revision 1.

[i.9] CCMB-2022-11-002: "Common Criteria for Information Technology Security Evaluation; Part 2: Security functional components", November 2022, Revision 1.

[i.10] CCMB-2022-11-003: "Common Criteria for Information Technology Security Evaluation; Part 3: Security assurance components", November 2022, Revision 1.

[i.11] FIPS 204: "Module-Lattice-Based Digital Signature Standard" (ML-DSA).

[i.12] FIPS 205: "Stateless Hash-Based Digital Signature Standard" (SLH-DSA).

[i.13] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.14] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access Control; Release 2".

[i.15] European Commission: "C-ITS Security - EU C-ITS security credential management system (EU CCMS)".

[i.16] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

ITS application: entity that defines and implements an ITS use case or a set of ITS use cases

ITS use case: specific scenario in which ITS messages are exchanged

ITS user: any ITS application or functional agent sending, receiving or accessing ITS-related information

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Attribute Authority
ABAC	Attribute Based Access Control
CAM	Cooperative Awareness Message
CRQC	Cryptographically Relevant Quantum Computer
DENM	Decentralized Environmental Notification Message
DTS	Dedicated Test System
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ExVe	External to Vehicle
FALCON	Fast Fourier Lattice-based Compact Signatures over NTRU
FEC	Forward Error Correction
IFI	In-Field Inspection
ITM	Infield Test Mode
ITS	Intelligent Transport System
ITS-S	ITS Station
MER	Message Error Rate
ML-DSA	Module-Lattice-based Digital Signature Algorithm
PKI	Public Keying Infrastructure
PP	Protection Profile
PTI	Periodic Technical Inspection
QoS	Quality of Service

RF	Radio Frequency
SLH-DSA	StateLess Hash-based Digital Signature Algorithm
SSP	Service Specific Permissions
SUT	System Under Test
SVI	Secure Vehicle Interface
ToE	Target of Evaluation
TVRA	Threat, Vulnerability and Risk Analysis
ZT	Zero Trust

4 The TVRA Method

The ETSI Threat, Vulnerability and Risk Analysis (TVRA) [i.1] is used to identify risks to a system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system.

In addition the present document applies parts of the ZT-Kipling Method described in ETSI TS 104 102 [i.6] in order to assist in identifying the role and purpose of assets in the system under evaluation.

For ease of use in translating the recommendations of the present document into a Protection Profile (PP) as may be required for certification purposes certain elements of the text are written in a Common Criteria [i.8], [i.9] and [i.10] relevant format.

The application of the TVRA method to specific applications is addressed in the present document in Annex A, addressing the threat of a Quantum Computing attack on cryptographic protections of ITS, and in Annex B, addressing the threat and impact of in-field testing mode on ITS operation.

Annex A:
Application Note - Quantum Computing attack on cryptographic protections of ITS

A.1 Overview of threat and form of attack

As outlined in ETSI EG 203 310 [i.3] all cryptographic algorithms should be considered to have a finite lifetime, where that lifetime is determined in part by advances in cryptanalysis, by advances in computing, and by advances in the underlying mathematical knowledge that underpins cryptology. In the domain of quantum computing there is a step change in the way that computing attacks on cryptographic algorithms will occur. With the advent of realizable Quantum Computers everything that has been transmitted or stored and that has been protected by one of the known to be vulnerable algorithms, or that will ever be stored or transmitted, will become unprotected and thus vulnerable to public disclosure. As the known to be vulnerable algorithms include those used in C-ITS/ITS the threat to C-ITS/ITS is considered in the present document.

The function of a quantum computer is summarized in Annex A of ETSI EG 203 310 [i.3] and a summary of each of Shor's and Grover's algorithms can be found in Annexes B and C respectively of the same document. For the purposes of the present document the threat or attack can be simplified to a statement that the existence of a viable quantum computer invalidates any security assertion made by existing asymmetric cryptographic technology, and specifically the primary quantum threat to Elliptic Curve Digital Signature Algorithm (ECDSA) as used in C-ITS is that a sufficiently powerful quantum computer could use Shor's algorithm to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) in polynomial time, allowing an attacker to calculate a private key from a public key. This would enable an attacker to forge the signatures that are used to build trust in the attribute attestations of C-ITS.

The threat can be written in a Common Criteria [i.8], [i.9] and [i.10] format as follows where the primary threat is masquerade as shown:

T.Masquerade: An attacker with a quantum computer and access to any public key certificate can determine the associated private key and masquerade as the private key holder

T.UnauthorizedOperation: An attacker with a compromised identity can perform operations with the privilege of the masqueraded identity.

NOTE: As the primary threat is that no presented identity is trustable given that a quantum computer can be used to recover the private key of any key pair then any subsequent use of the compromised identity is secondary and only by removal of the masquerade threat can the system be restored to normal operation.

A.2 Scope of a quantum computing attack in ITS

Following the practice of ETSI TS 102 165-1 [i.1] to identify the assets in the system and their interactions that are impacted by a particular attack the present document asserts the following:

- All cryptographic assets, technical operations, stores and management operations of the ITS system are impacted.

The assessment made in ETSI TR 103 949 [i.5] is that where C-ITS/ITS uses elliptical curve cryptography there is a substantial risk of masquerade (impersonation attack) and that can lead to collapse of the required trust model. ETSI TR 103 949 [i.5] only explicitly analysed the keying infrastructure and then implicitly the application of cryptographic operations that are dependent on that infrastructure. The attack considered is the application of a quantum computer in such a way that any public key certificate can be processed to recover the matching private key. Once a private key is recovered there is no way to determine the authenticity of anything protected by that private key.

A.3 Impact of the quantum computing attack in ITS

The assessment of the impact to ITS and C-ITS as a whole by the existence of a Cryptographically Relevant Quantum Computer (CRQC) is that it is High. 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.

A.4 Risk assessment of quantum computing attack in ITS

Applying the risk model from ETSI TS 102 165-1 [i.1] there is some uncertainty 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 A.1).

Table A.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.

A.5 Countermeasure considerations for quantum computing attack on ITS

The risk to ITS of a Quantum Computer applied to the keying infrastructure is critical and the mitigation is non-trivial. Whilst quantum safe cryptographic algorithms exist they require substantially more bandwidth than any current algorithm. This addresses not just signature and key sizes for transmission but also the processing required to create and verify signatures.

Whilst C-ITS/ITS systems generally have been designed with crypto-agility in mind the scale of ITS systems, having very large numbers of stakeholders and a considerably larger number of impacted devices, requires that migration to a post quantum environment (i.e. one that is fully quantum safe) is considered as a critical task. The process of migration is described in ETSI TR 103 619 [i.4] and for ITS in ETSI TR 103 949 [i.5].

All ITS-Ss will be required to be Quantum Safe.

A.6 Specific considerations for QSC in C-ITS

A standard ECDSA signature size is approximately twice the length of the underlying elliptic curve's key size, or approximately 64 bytes (512 bits) for a 32 byte (256-bit) curve. The performance requirement identified in ETSI TS 103 300-2 [i.7] and stated in clause 5.3.3 of [i.7] as OSEC01 "*The security processes shall support generating messages at a rate of 10 Hz, receiving messages at a rate of 2 KHz, latency of 300 ms end-to-end and an average sent packet size over 1 s of 300 bytes*". Each message is assumed to be signed and the verification key available, this means 2 000 signature verifications per second, and 10 signature creations per second. The channel capacity at 5,9 GHz for C-ITS is not particularly impacted (the 10 MHz channels can comfortably cope with several 10 s of Mb/s of data traffic) although with normal radio conditions the more data that is contained in a packet the greater the chance of packet loss even with reasonably robust Forward Error Correction (FEC) added at lower layers. C-ITS is predicated on a datagram transmission protocol with no linkage between transmitted packets and the QoS is defined as best effort all informed, particularly for CAM (i.e. all messages are broadcast and there is no verification of receipt).

QSC signature algorithms have signature sizes that are often several orders of magnitude greater than conventional signatures (e.g. RSA, ECDSA). Thus, as an example using a Lattice based signature scheme such as Falcon with a 666 byte signature size the assumptions underpinning OSEC01 from [i.7] cannot be met with a direct replacement of ECDSA with a QSC signature.

In ETSI TR 103 949 [i.5] the prognosis was not identified as good. The assessment of algorithms where the intent is to migrate from the ECDSA algorithm and its associated keys to an equivalent strength quantum safe algorithm with a review of the applicability of some of the NIST assessed algorithms is given in Table A.2 (note that this is an update of Table 7 from [i.5]) against the expectations of ITS/C-ITS.

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 A.2 identifies parameter and signature size against NIST security category 2 (ML-DSA-44), and security category 1 (FALCON and each of SLH-DSA-SHA2-128f and SLH-DSA-SHA2-128s).

NOTE 3: There are 5 identified NIST Post Quantum Security categories. Category 1 is defined as having resistance equivalent to exhaustive key search of AES-128, category 2 is defined as equivalent to the collision resistance of SHA256, category 3 as equivalent to AES-192, category 4 as equivalent to collision resistance of SHA-384, and category 5 as equivalent to AES-256.

Table A.2: NIST list of quantum safe signature algorithms (published or under pre-publication review)

Algorithm	Outline	Signature size	Key sizes	Suitability to ITS
ML DSA FIPS 204 [i.11]	Recommended by NIST as a primary algorithm.	2 420 bytes ML-DSA-44 (L2)	Public 1 312 bytes Private 2 560 bytes ML-DSA-44 (L2)	No. The signature size is significantly in excess of the payload capacity of the G5 radio link.
Fast Fourier Lattice-based Compact Signatures over NTRU (FALCON) (FIPS 206 draft)	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.	666 bytes FALCON-512 (L1)	Public 897 bytes Private 1 281 bytes FALCON-512 (L1)	Marginal as the signature size is at the absolute limit of G5 capacity. It is reported that Falcon signing is hard to implement in a fast and timing side-channel secure manner.

Algorithm	Outline	Signature size	Key sizes	Suitability to ITS
SLH-DSA FIPS 205 [i.12]	Noted by NIST as a backup as the mathematical basis is different from the others. FIPS 205 [i.12] is based on conventional hash algorithms (SHA256) but in a very complex set of structures.	SLH-DSA-SHA2-128f: 17 088 bytes (L1) SLH-DSA-SHA2-128s: 7 856 bytes (L1)	Public 32 bytes Private 64 bytes (L1)	No. The signature size is significantly in excess of the payload capacity of the G5 radio link.

As Table A.2 makes clear the Quantum Safe Signature algorithms identified by NIST for standardization yield signatures that exceed the viable 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.

NOTE: A consequence of increasing the packet size in any radio transmission is that the error behaviour is changed with either a higher power envelope being required, a reduction in range, or more advanced FEC applied if the same Message Error Rate (MER) is to be maintained. As transmission range per unit of power decreases as the transmission frequency increases, and as the C-ITS/ITS transmissions are subject to strict restrictions on power levels there is no obvious leeway to modify transmission power to maintain MER, nor is there opportunity to add more robust FEC to the base system to maintain MER. The consequence therefore is that if the transmission packet size is increased the operational range for a given MER will decrease.

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. There is no significant advantage in waiting for an ideal algorithm to be developed as that severely impacts on the time factors 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. This is a direct consequence of the requirement for pseudonymity arising from a desire to reduce the risk of tracking and thus the creation of short lived key pairs. 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 A.3 gives estimates of the capacity required for such a transmission, excluding the payload itself (note that Table A.3 is an update of Table 8 from [i.5]).

Table A.3: Estimated capacity required in C-ITS messages

Algorithm	Estimated capacity required in C-ITS messages
ML DSA FIPS 204 [i.11] (ML-DSA-44)	6 152 bytes (2 of 2 420 byte signatures, 1 of 1 312 byte public key)
FALCON (FALCON-512)	2 229 bytes (2 of 666 byte signatures, 1 of 897 byte public key)
SLH-DSA FIPS 205 [i.12] (SLH-DSA-SHA2-128f)	34 208 bytes (2 of 17 088 byte signatures, 1 of 32 byte public key)

Whilst it is recognized that the operational attestation model uses short lifetime keys this does not offer a path to avoid the complications of making the system quantum safe. However in a hybrid model the attestations made by an ITS-S could be based on existing non-QSC mechanisms only if the AA and AT entities migrate to a QSC scheme. The value of the short life keys and the masquerade opportunity to an attacker is less useful. All long lifetime keys from AAs and ATs, as they are root authorities and the AA public keys should be well known to all ITS-S as they are used to verify the attestations of any individual transmission (i.e. the logic is that an attestation of a transmitting ITS-S is authorized by the AA and the AA is considered a persistent system entity) have to use QSC.

A.7 QSC support by modification of the C-ITS security model

As noted in ETSI TR 103 619 [i.4] 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, the remainder of this annex examines the veracity of the assumption.

The ITS communications model has a complex set of roles and responsibilities. Communication may be from an external party to access vehicle resident data, e.g. OnBoard Weighing, or for remote control, e.g. Valet Controlled Parking. The ITS security model is based on access to data being privileged and therefore the primary model is Attribute Based Access Control (ABAC) with some qualifications. For CAM messages, the ones identified in clause 5.3.3 of ETSI TS 103 300-2 [i.7], the authority to process is based on the message coming from an ITS-S known to, and authorized by, a trusted AA. The message itself is pseudonymous, i.e. it has no persistent Personal Identifying Information. Ideally no two messages from the same transmitting party should be linkable. If the AA attests that the transmitter is to be trusted for a specific role then that message can be consumed. Each message is signed by the transmitter with the CA for each signature being the appropriate (role specific) AA.

The ITS/C-ITS model has very few security associations that can be managed in advance, hence the only reasonable cryptographic model is one using public key cryptography. However how PKC is used can be reconsidered to maximize efficiency. Furthermore there is no significant use of persistent connections in ITS/C-ITS and those that do exist (e.g. those requiring access to on-vehicle data or processes) are between unknown parties where public key cryptography is the only reasonable tool to initiate a secure connection (where the connection may be secured by shared symmetric key cryptography).

As has been identified in ETSI TR 103 949 [i.5] there are large infrastructures in support of ITS/C-ITS operation, exemplified by the models shown below (copied from Annex C of [i.5]).

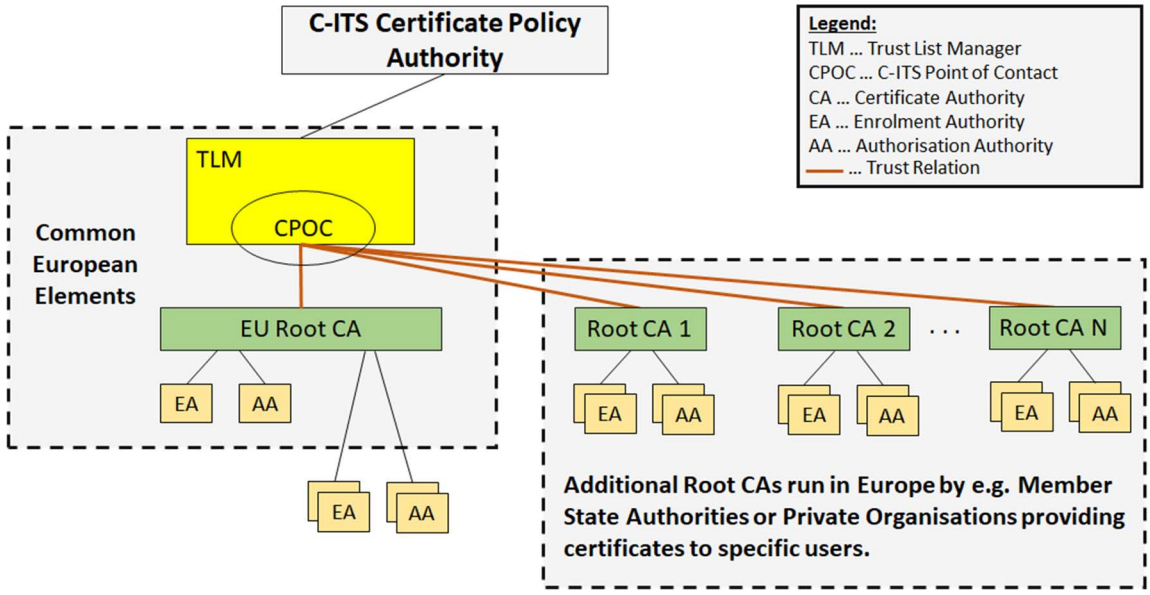
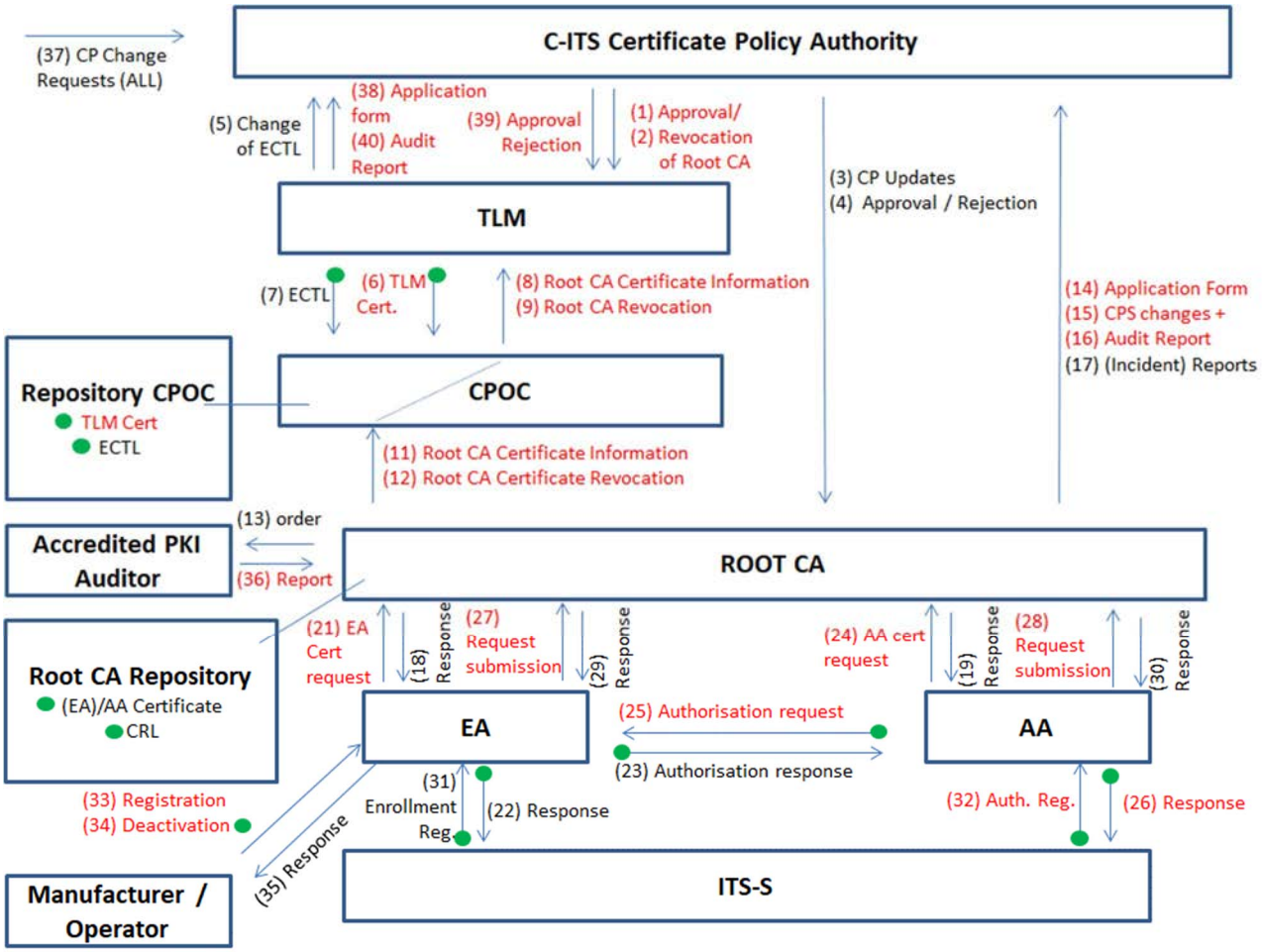


Figure A.1: EU CCMS basic model



NOTE: The numbered sequences shown above are defined in the EU CCMS [i.15] documentation and not copied here.

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

Migration to a QSC solution has to address the infrastructure elements first. The model in all PKIs is that it is a top down model, trust rolls from the top of the stack, i.e. the Certificate Authority, to the end point. Trust verification moves from the bottom of the stack to the top. Pre-installing the public keys and their certificates of as many layers of the hierarchy as possible into each end-point may improve speed but has a risk of missing revocation notices if immediate online confirmation of the integrity of the PKI itself is not performed on a regular (and frequent) schedule.

NOTE 1: For ITS deployments it may be conceived that each CA-EA-AA group could migrate independently but the coordination through the Trust List Manager then may become more complex, particularly if an ITS-S attaches to multiple branches.

For C-ITS where the purpose is to share information on the location of vehicles (represented as ITS-Ss using CAMs) and for the event notifications (using DENMs) the datagram model carrying proof of authorization using a public key signature countersigned by the AA remains appropriate. For the use cases represented by SVI and ExVe (see Annexes D and E of [i.5]) the migration of TLS to a quantum safe mode should suffice and an appropriate cryptosuite selected.

NOTE 2: The current set of cryptosuites for TLS that are identified in the ClientHello message do not include full QSC capability.

Annex B:
Application Note - Impact of in-field testing mode on ITS operation

B.1 Overview of threat and form of attack

The Infield Test Mode (ITM) for C-ITS addresses a number of use cases that are summarized below:

- Repair and maintenance in authorized workshops:
  - Within an authorized workshop (a fixed building), the ITM is used to identify corruption of the ITS-S and may include testing of the RF-equipment, and then to validate it after repair, maintenance, or change of components, has been completed. Therefore the ITS-S acting as the System Under Test (SUT) will interact with a Dedicated Test System (DTS).
- Periodic Technical Inspection (PTI):

EXAMPLE: PTI includes the road-worthiness tests carried out in most countries, e.g. the MoT test in the UK, the Contrôle Technique in France, the Hauptuntersuchung (HU) (often called a TÜV) in Germany.

  - During PTI the ITM is used for functional validation of SUT C-ITS communication components.

NOTE: The currently sanctioned government PTIs do not normally include a "road test", rather they are workshop based tests and the vehicle is generally stationary (exceptions are allowed but generally the test is not performed on public roads).

- In-Field Inspection (IFI):
  - The In-Field Inspection is a verification of SUTs in the field and a maintenance of network quality where the SUT and the ITM-DTS is performed by specially authorized entities.
- Perception Test (PT):
  - The Perception Test is a verification to help identify problems linked to sensors feeding data into the ITS messages that are visible at system level but not at ITS-S level. To perform this perception test, the DTS has knowledge of the potential perceived objects and areas by the SUT, using a selection of the sensors. For example, the test environment can use other vehicles or a fake scene for which the SUT should provide perceived objects or areas in the test response. The DTS sends a perception test request message containing the list of selected sensors to the SUT requesting a perception test response. The requested sensors may be selected according to their identifiers, types, ranges, position and field-of-views.
- Other Scenarios:
  - An unauthorized user is using a transceiver radio device in order to trigger the ITS-S (SUT) to change its mode to ITM by trying any kind of malicious messages.
  - An unauthorized user tries to gain access to an ITS-S (SUT) for inserting a self-generated root certificate. By using this certificate it might be possible to start a unauthorized ITM communication between the unauthorized DTS and the SUT.

In any conventional system it is assumed that devices are tested and determined as ready to be placed on the market, often using random samples of devices, and that the device once placed on the market has no requirement for supporting any mode of operation that is a "test mode", or "test configuration". In contrast ITM specifically enables a test mode that provides the ability to test the ITS-S (acting as an SUT). The scope of testing includes Radio Frequency (RF) and functional requirements of devices whilst in non-shielded environments. The immediate consequence is that those ITS-Ss in test mode have to be isolated by design from any operational stations. As C-ITS operation is predicated on all informed broadcast there is a requirement to ensure that test mode does not interfere with normal C-ITS operation.

The primary risk is to enable test mode without clear operational separation of duties.

The threats of ITM can be written in a Common Criteria [i.8], [i.9] and [i.10] format as follows where the primary threat is unauthorized operation as shown:

T.UnauthorizedOperation: An attacker enables ITM mode to remove ITS-Ss in a target area from normal operation.

As unauthorized ITM may place vehicle operators at significantly increased risk (through loss of direct control of the vehicle in the extreme case) the impact should be evaluated as High. Without due attention to mitigation, and noting as described below that the key elements of C-ITS/ITS remain identical to non-ITM operation, there is at least moderate likelihood of unauthorized operation.

B.2 Identification of delta Target Of Evaluation (TOE)

The ToE is defined by the system and its environment shown in Figure B.1 which extends the base ToE with the addition of an ITS-S acting as the DTS. The purpose of this system is the evaluation of an ITS-S concerning its conformance to existing test suites with the operation of those test suites being post deployment and with the ITS-S in the operational environment, rather than in the conventional case where conformance tests are carried out in a laboratory setting. In this overall view the SUT and its communication partners are considered as the ToE.

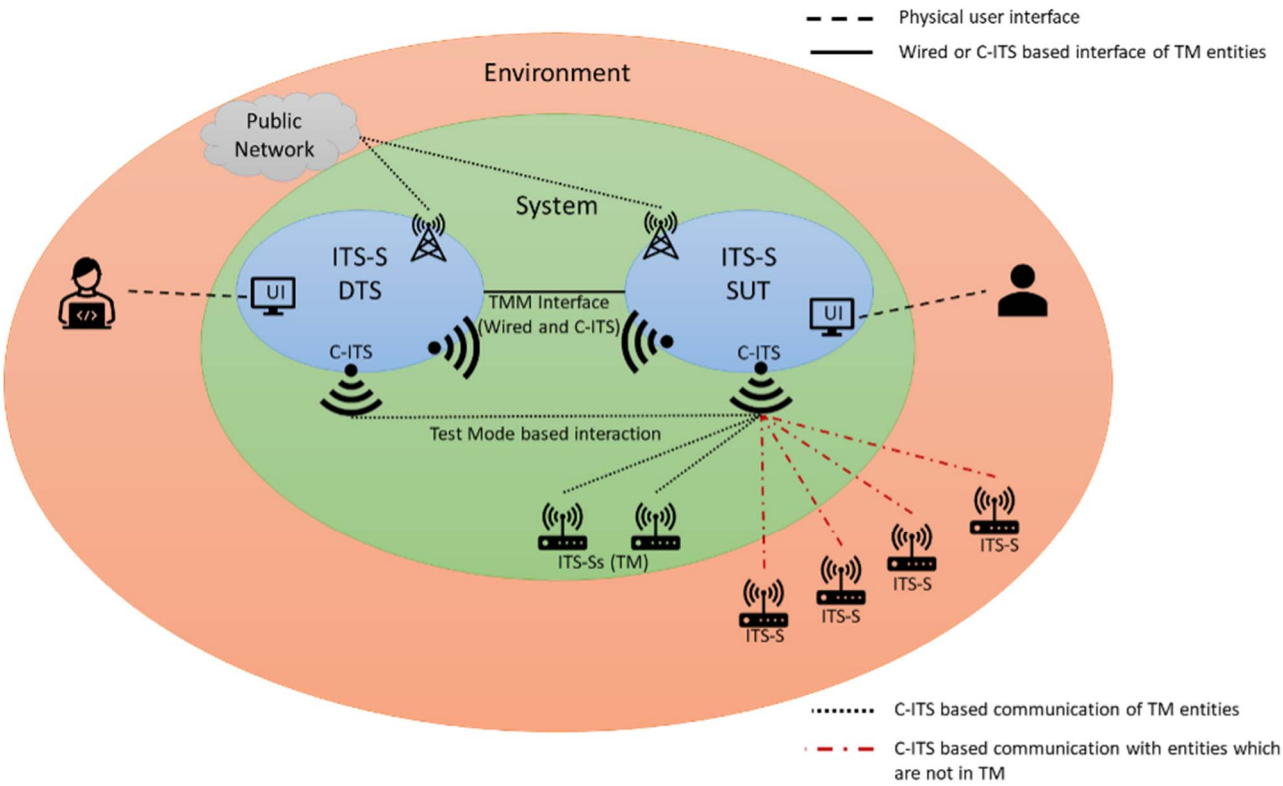


Figure B.1: ToE for TVRA of ITM

The interfaces of the DTS and the SUT represent potential attack interfaces. Those interfaces are functionally identical to an ITS-S in normal operational mode (this is essential as the ITM is intended to test those interfaces (physical and logical) and the processes and features the give access to).

This gives rise to the first substantial recommendation:

- ITM should be logically distinct from any normal mode of operation and normal operation should be suspended.

NOTE 1: This requires that when an ITS-S is operating in ITM it will not send conventional C-ITS messages and should not process any received conventional C-ITS messages (i.e. it will only respond to stimuli from the DTS).

By enforcing logically distinct operation it further suggests that the following recommendation is enforced:

- ITM should be cryptographically distinct from any normal mode of operation and normal operation should be suspended.

NOTE 2: The above recommendation in turn requires that the Certificate Authority (CA) for ITM (i.e. the EA, AA) are distinct and that any stored cryptographic material for normal modes of operation are suspended whilst in ITM.

As ITM is a functional test of the ITS-S (the SUT) it cannot use different interfaces or frequencies. With limited control of the reach of a radio based ITM there is a risk of "leakage" of ITM test messaging into the normal ITS environment. In light of the risk of ITM leakage the preferred mode of ITM should be with the RF elements disabled, thus access to the ITS-S should be from a dedicated test port. In such cases the RF elements should be able to be discretely tested.

NOTE 3: In deployment the core recommendations from ETSI EN 303 645 [i.13] apply, in particular the provisions to minimize attack surfaces. In ITM only the essential interfaces required for any particular test should be open.

B.3 Identification of security objectives

B.3.1 Purpose

The purpose of ITM is to conduct tests on the equipment (the ITS-S acting as SUT), not on the wider system. Thus the primary objective is that ITM, and all affected equipment (ITS-S, DTS, etc.) is isolated cryptographically and operationally from any operational ITS system.

For the purpose of ITM the DTS is an ITS-S acting as a source or sink of ITS messages.

From a functional safety viewpoint the ITM mode should not place any operator of equipment at increased risk than from operating the ITS-S than when in normal operational mode.

NOTE: Many of the conformance tests defined for ITS/C-ITS require that a human tester observes or stimulates the system. If the SUT is present in a vehicle then the human tester cannot be distracted from operation of the vehicle and therefore any tests that may give rise to such interference should only be conducted with the human tester as a passenger and not as the vehicle operator.

B.3.2 Confidentiality

The confidentiality objectives and requirements for non-ITM apply.

NOTE: As ITM is not the same as diagnostic testing of the vehicle to which an ITS-S is attached the level of private data in an ITM session should be identical to that in any other session thus the same confidentiality provisions as for normal ITS/C-ITS should apply.

B.3.3 Integrity

The integrity objectives and requirements for non-ITM apply.

NOTE: As a message in normal (non-ITM) sessions has a signature generated over the content, and the signature verifies both the authenticity and integrity of the message, and the message structures are unchanged for ITM, then the integrity provisions as for normal ITS/C-ITS should apply.

B.3.4 Authenticity

The authenticity objectives and requirements for non-ITM apply.

NOTE: As a message in normal (non-ITM) sessions has a signature generated over the content, and the signature verifies both the authenticity and integrity of the message, and the message structures are unchanged for ITM, then the authenticity provisions as for normal ITS/C-ITS should apply.

B.3.5 Availability

The availability objectives and requirements for non-ITM apply with the following extension (see also clause B.6):

- ITM should be a specific authorized service from an AA.

B.4 Quantitative risk analysis for ITM

The risk calculated from the combination of impact and likelihood of a successful attack on an ITS-S is given as below:

- Impact - High.
- Likelihood - Moderate to High.
- Assessed risk - Major to Critical.

The impact is considered as invariant as outlined in clause B.1 and assessed as high because unauthorized placement of an ITS-S (and by consequence the vehicle it is mounted in) as significantly changed risk from normal ITS operation. In assessing the likelihood the assessment is initially made with only normal ITS measures in place and no special provisions for ITM being available. In this case the ability to distinguish an ITM message from any other (assuming validity of the AA cert) is low. If, however, the design practices identified in ETSI EN 303 645 [i.13] are followed and a conservative approach to access control is taken the likelihood may be more managed and reduce from a high likelihood to moderate likelihood. The provision of the countermeasures in clause B.5 bring the likelihood down to low and risk to Major (as the impact is invariant).

B.5 Security countermeasure identification

For each of the identified threats it is necessary to consider what countermeasures can be implemented to reduce the risk of an attack being successfully mounted on an ITS-S and its impact. The TVRA is only intended to provide an estimation of possible countermeasures for the above-mentioned threats with regard to previous assets, it should be noted that not all measures can be applied to every hardware platform and may involve greater effort to implement. An assessment of which countermeasures will be mandatory for ITM and which are advisory is out of scope.

The primary threat identified in clause B.1 is "***T.UnauthorizedOperation*** *An attacker enables ITM mode to remove ITS-Ss in a target area from normal operation*". In order to mitigate this threat the system has to be able to successfully prevent unauthorized operation. The core access control model of ETSI TS 102 942 [i.14] is ABAC and one of the purposes of ABAC is to ensure that any data or process of the ITS-S and its associated environment is only accessible by authorized entities. The default condition of the ABAC model in ETSI TS 102 942 [i.14] is DENY, thus only positively identified ITM messages can be consumed and able to access the necessary resources of the ITS-S.

The following requirements apply to the ABAC model for enabling ITM:

- All messages exchanged in ITM mode have to be countersigned by an AA acting as an ITM Authority:
  - An ITM Authority is expected to have further restrictions as identified in the use cases in B.1, for example PTI, IFI.
- ITM mode of an ITS-S is a protected resource.

NOTE 1: For use case PTI the inspecting workshop and the authority it is enabled by should be identifiable.

NOTE 2: Invocation of PTI should not be able to change any parameters of the ITS-S and its associated environment but should only be able to enable reporting of data elements.

The application of the ZT-Kipling method [i.6] may be used to assist in the definition of rules and policies for the access control model for ITM. An example of the application of the method is given in Table B.1 below.

Table B.1: Application of ZT-Kipling criteria for ABAC in enabling ITM

Kipling criteria	Example for ITM invocation
What	Is the ITS-S enabled for ITM?
Why	Is ITM appropriate at this time? If vehicle is moving then deny
When	Is the time of the ITM invocation valid based on the current time of the ITS-S?
How	How is the invocation verified>
Where	Is the geo-location of the ITM invocation valid based on the current location of the ITS-S?
Who	Who is invoking ITM?

History

Version	Date	Status
V2.1.1	May 2026	Publication