Technical Specification

ISO/TS 5616

First edition
2024-12

Intelligent transport systems — Secure interfaces governance — Minimum requirements and governance procedures

Systèmes de transport intelligents — Gouvernance à l'aide d'interfaces sécurisées — Exigences minimales et procédures de gouvernance

Reference number
ISO/TS 5616:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides specifications for the minimum requirements for a governance process for using "ITS Trusted Devices" for ITS data management and access via secure interfaces.

The paradigm presented in this document can be used for any ITS interface, but it is particularly focused on meeting some of the unique characteristics of the interface between a vehicle and external entities, such as roadside units and other vehicles.

While many technical specifications and standards have already been developed on the use of ITS devices for ITS data management and access (and on which this document relies), combinations of such documents need to be used consistently and the whole system needs to be consistently governed. This document concerns the adoption and use of combinations of existing approved technical specifications or standards in combination with governance processes. It does not introduce new technical specifications. While it enables government policies to be consistently supported, it does not specify those policies.

For the purposes of this document, the term "governance" encompasses the use and combination of systems that direct and control ITS data entities, including the structure and processes for decision making, accountability, control and behaviour. ITS data governance influences how an organization’s objectives are set and achieved, and how risk is monitored and addressed in terms of the acquisition, use, retention, sharing and elimination of ITS data. ITS data governance also prescribes a system and a process, rather than a single activity; successful implementation of a good governance strategy therefore requires a systematic approach that incorporates strategic planning, risk management and performance management.

The purpose of this document is to specify the use and combination of (largely already existent) standards and specifications for the governance of data across ITS secure interfaces, and to present organizational concepts to support such governance measures in accordance with the principles of ISO/TC 204 policy documents concerning ITS data governance policy. This involves the components of a so called "trust model" [e.g. PKI (public key infrastructure) services] as well as the entities running them, i.e. the trusted third parties for the trust and privacy management on which operational entities rely, and which allow them to be run in a secure and reliable way.

Governance in an international context and covering a wide range of use-case paradigms with different needs necessitates a multi-layer governance model, with general governance and specification of high-level options that are useable by all and maintain consistency. Regional requirements can be introduced to this level to meet the needs of regional government.

These operational aspects need be overt and clear to all and provide the principal policy requirements and options to maintain cybersecure interoperability. They can be found in accordance with the principles of ISO/TC 204 policy documents concerning ITS data governance policy and form the principle recommendations and minimum requirements for governance of ITS data management and access. However, many aspects refer to and provide links to published government policy deliverables, so while they can be referenced in ISO/TC 204 ITS data policy documents, they are not suitable for inclusion in an ISO standards deliverable. This document is focused on the generic minimum interoperability requirements and general procedures for governance to maintain consistency for ITS data management and access.

To complicate issues, there is no monolithic model that can be applied in exactly the same way in all regions of the world. Yet, consistent governance needs to operate consistently within the differing policy requirements of governments around the world, within a framework where governments can agree on common interoperable policies, whilst achieving their own objectives and requirements.

A second regional level of governance determines the options allowed within a region for each defined application domain (e.g. service group).

This lower level of governance is at the operational level, determining the choice of the options allowed in order to meet the application needs.

Application domains/service groups can operate solely within one region, or can operate in multiple regions or globally, in which case they can have to specify different and multiple operational specifications to meet different regional requirements.

These aspects need to be in accordance with the principles of ISO/TC 204 policy documents concerning ITS data governance policy that detail general principles of governance and the aspects that have to be considered in such policymaking. However, the options specified are taken at this operational level, ratified by the regional governance management committee (RGMC), and not by this document.

To visually summarize such a governance paradigm, Figure 1 shows a conceptual governance reference architecture, as elaborated in accordance with the principles of ISO/TC 204 policy documents concerning ITS data governance policy.

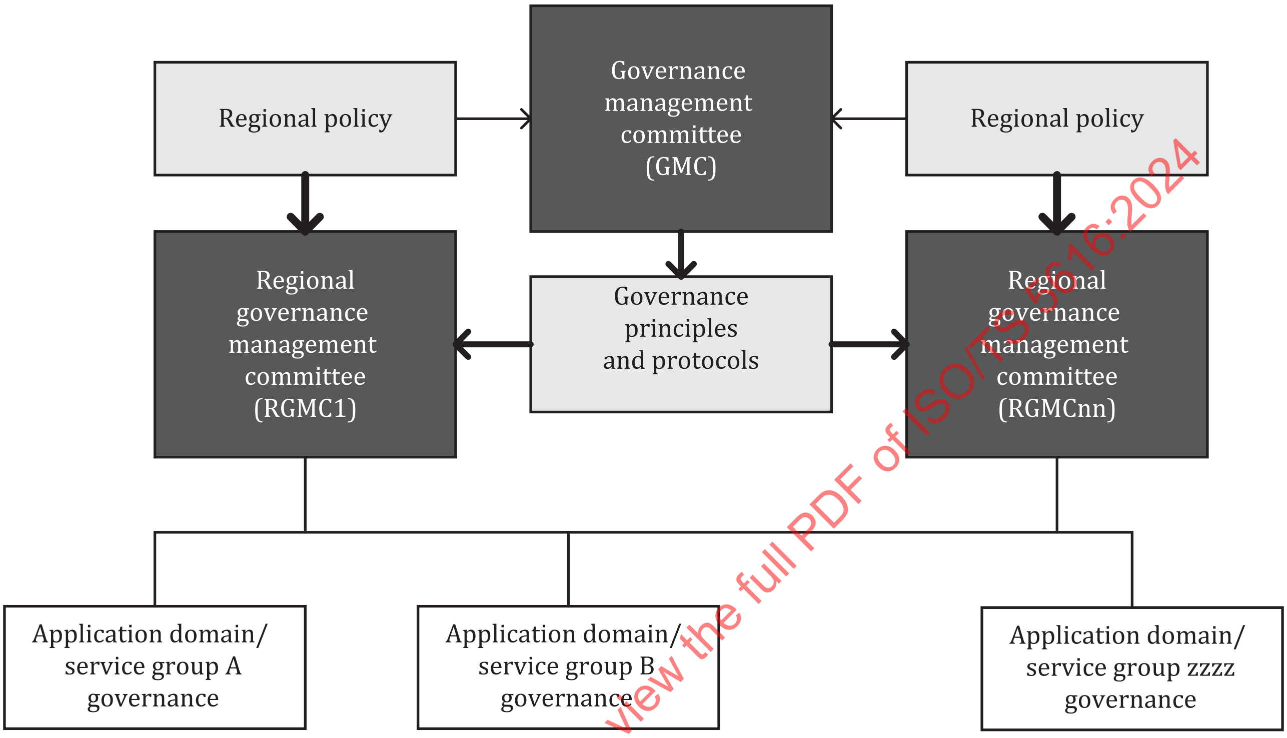

Regional policy
Governance management committee (GMC)
Regional policy
Regional governance management committee (RGMC1)
Governance principles and protocols
Regional governance management committee (RGMCnn)
Application domain/ service group A governance
Application domain/ service group B governance
Application domain/ service group zzzz governance

Figure 1 — Conceptual governance reference architecture

This document provides the minimum requirements to be met in order to achieve interoperability and consistent governance, while enabling governments to implement their policy decisions.

This document specifies a generic framework to enable a consistent governance process for using "ITS Trusted Devices" for ITS data management and access using secure interfaces, but is not concerned with and does not determine the policy decisions that the governance process potentially make, nor the wireless media nor media protocols used to conduct communications.

Intelligent transport systems — Secure interfaces governance — Minimum requirements and governance procedures

1 Scope

This document specifies the minimum governance procedure requirements for ITS data management and access using secure interfaces (and, particularly, secure vehicle interfaces) in order to meet objectives in accordance with the principles of ISO/TC 204 policy documents concerning ITS data governance policy.

NOTE 1 Where an ITS data management and access paradigm is already in existence, this document proposes only to provide a suitable checklist for any assessment of its competency. This document does not propose that existing arrangements that are acceptably competent be changed.

NOTE 2 This document does not affect proprietary original equipment manufacturer (OEM) communications using ExVe (see ISO 20077-1), but does provide means for its complementary coexistence.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 15031-2, *Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 2: Guidance on terms, definitions, abbreviations and acronyms*

ISO 18541-1,, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 1: General information and use case definition*

ISO 18541-2, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 2: Technical requirements*

ISO 18541-3, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 3: Functional user interface requirements*

ISO 18541-4, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 4: Conformance test*

ISO 20077-1, *Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information*

ISO 21177, *Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices*

ISO/TS 21184, *Cooperative intelligent transport systems (C-ITS) — Global transport data management (GTDM) framework*

ISO/TS 21185, *Intelligent transport systems — Communication profiles for secure connections between trusted devices*

ISO 21217,, *Intelligent transport systems — Station and communication architecture*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ETSI/TS 103 097, *Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1 General terms used in this document

3.1.1
access
right to and ability to obtain data in a defined and limited context

3.1.2
actor
participant, person or organization who does something relevant in the system

3.1.3
domain
specified sphere of activity

3.1.4
extended vehicle
ExVe
physical road vehicle with external software and hardware extensions for some of its

features

Note 1 to entry: These extensions are developed, implemented and managed by the vehicle manufacturer who is fully responsible for the communication among the various parts of the extended vehicle, especially between the internal and external software and hardware components.

3.1.5
governance
concept referring to the actions and processes by which stable practices and organizations arise and persist

Note 1 to entry: The term "governance" encompasses the use and combination of systems that direct and control ITS data entities, including the structure and processes for decision making, accountability, control and behaviour. ITS data governance influences how an organization's objectives are set and achieved, how risk is monitored and addressed in terms of the acquisition, use, retention, sharing and elimination of ITS data. It prescribes a system and a process, not a single activity. Successful implementation of a good governance strategy therefore requires a systematic approach that incorporates strategic planning, risk management and performance management.

3.1.6
governance management committee
GMC
high-level body comprised of RGMC representatives responsible for the governance of ITS Data management and access that determine global policy and regional variations

3.1.7
information security
preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2017, 3.28]

3.1.8
infrastructure
system of facilities, equipment and applications needed for the operation of an organization that provides ITS services that use fixed ITS trusted devices

3.1.9
ITS data
data associated with transport systems that is transferred, often wirelessly, from one system to another and/or used within a system in order to provide an ITS service

3.1.10
ITS trusted device
device which cooperates with another device in a trusted way, i.e. exchange of information with optional explicit bi-directional protection

Note 1 to entry: See ISO 21217 for further information.

3.1.11
ITS-station
instance of an ITS trusted device operating as a functional entity, comprised of an ITS-S facilities layer, ITS-S networking and transport layer, ITS-S access layer, ITS-S management entity, ITS-S security entity and ITS-S applications entity providing ITS services

Note 1 to entry: From an abstract point of view, the term “ITS station” refers to a set of functionalities. The term is often used to refer to an instantiation of these functionalities in a physical unit. Often the appropriate interpretation is obvious from the context. The proper name of the physical instantiation of an ITS-S is ITS station unit (ITS-SU)

3.1.12
paradigm
model, or a very clear and typical example, of a system, situation or environment

3.1.13
public key infrastructure
PKI
set of roles, policies, hardware, software and procedures to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption

Note 1 to entry: This is an arrangement that binds public keys with respective identities of entities (like people and organizations).

Note 1 to entry: The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).

3.1.14
regional governance management committee
RGMC
body responsible for governance of ITS data management and access in a defined geographic region

3.1.15
role
position or purpose that someone or something has in an organization, society or relationship

3.1.16
secure interface
cybersecure bidirectional communication connection (wired or wireless) between two entities known as "ITS-stations"

Note 1 to entry: "ITS-stations" are defined in 3.1.13 and in ISO 21217.

3.1.17
secure vehicle interface
secure interface in which at least one of the parties is a connection to a vehicle

3.1.18
subject
natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber

3.1.19
subscriber
natural person or legal entity (applicant) to which a certificate is issued and that is legally bound by a subscriber agreement or terms of use agreement

3.2 Recommended definitions for certificate policy (Annex A)

3.2.1
applicant
natural person or legal entity that applies for (or seeks renewal of) a certificate

Note 1 to entry: Once the initial certificate is created (initialization), the applicant is referred to as the "subscriber".

Note 2 to entry: For certificates issued to end-entities, the subscriber (certificate applicant) is the entity that controls or operates/maintains the end-entity to which the certificate is issued, even if the end-entity is sending the actual certificate request.

3.2.2
authorization authority
AA
legal and/or operational entity managing authorization

Note 1 to entry: Within this document, the term "authorization authority" can also refer to the specific function of the AA (authorization authority).

3.2.3
certification authority
CA
legal and/or operational entity managing certification

Note 1 to entry: The root certification authority, enrolment authority and authorization authority are cumulatively referred to as the "certification authority" (CA).

3.2.4
crypto-agility
capability of the ITS-data "trust model" entities to adapt the certificate policy to changing environments or to new future requirements, e.g. by a change of cryptographic algorithms and key length over time

3.2.5
cryptographic module
secure hardware-based element within which keys are generated and/or stored, random numbers are generated, and data are signed or encrypted

3.2.6
enrolment authority
authority in the ITS PKI (public key infrastructure) structure that authenticates an ITS-S and grants it access to ITS communication which can be made pseudonymous by authorizing access to relevant AAs (authorization authorities) to grant authorization for specific services

3.2.7
ITS-data trust model
model responsible for establishing a relationship of trust between ITS trusted devices

Note 1 to entry: It is implemented through the use of a PKI (public key infrastructure) composed of root CAs (certification authorities), the ITD-POC (ITS data point of contact), TLM (trust list manager), EAs (enrolment authorities), AAs (authorization authorities) and a secure network.

3.2.8
PKI participants
public key infrastructure participants
entities of the ITS-data trust model, i.e. the TLM (trust list manager), root CAs (certification authorities), EAs (enrolment authorities), AAs (authorization authorities) and C-ITS (central ITS) stations

3.2.9
re-keying
subcomponent used to describe certain elements relating to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key

3.2.10
repository
entity used for storing the certificates and information on certificates provided by the entities of the ITS-data trust model

3.2.11
root certification authority
root CA
legal and/or operational entity managing root certification

Note 1 to entry: Within this document, the term "root certification authority" can also refer to the specific function of the root CA.

3.2.12
subject
natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber

3.2.13
subscriber
natural person or legal entity to which a certificate is issued and that is legally bound by a subscriber or terms of use agreement

3.2.14
subscriber agreement
agreement between the CA (certification authority) and the applicant/subscriber that specifies the rights and responsibilities of the parties

3.3 Recommended definitions for security policy (Annex A)

3.3.1
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.3.2
confidential information
information that is not to be made available or disclosed to unauthorized individuals, entities or processes

3.3.3
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[SOURCE: ISO/IEC 27000:2018, 3.31]

3.3.5
integrity
property of accuracy and completeness (ISO 27000)

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.3.6
ITS trusted device infrastructure
system of facilities, equipment and applications needed for the operation of an organization that provides services related to fixed ITS trusted devices

3.3.7
ITS rusted device stakeholders
individual, group or organization with a role and responsibility in the ITS trusted device network

3.3.8
local dynamic map
LDM
in-vehicle ITS trusted device station’s dynamically updated repository of data relating to local driving conditions

Note 1 to entry: The LDM includes information received from on-board sensors and from Cooperative Awareness Messages (CAMs) and Descentralized Evironmental Notification Messages (DENMs). See ETSI/TR 102 893.

3.3.9
protocol control
assets which select an appropriate message transfer protocol for an outgoing message request and send the message to the lower layers of the protocol stack in a format that can be processed by those layers

Note 1 to entry: Incoming messages are converted into a format that can be handled within the ITS trusted device and passed to the relevant functional asset for further processing. See ETSI/TR 102 893.

4 Abbreviated terms

4.1 General abbreviated terms used in this document

C-ITS	cooperative ITS
CMS	credential management system
CS	commissioning secretary
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
GMC	governance management committee
ITS	intelligent transport system(s)
ITS-S	ITS-station
ITS-SU	ITS-station unit
NAFTA	North America Free Trade Agreement
OEM	original equipment manufacturer
PKI	public key infrastructure
PMC	policy management committee
RGMC	regional governance management committee
SCMS	security credential management system

4.2 Recommended abbreviated terms for certificate policy

The following abbreviated terms are not necessarily used in this document but are recommended for use when elaborating certificate policy. See Annex B.

AA	authorization authority
AT	authorization ticket
CA	certification authority
CP	certificate policy
CPA	certificate policy authority
CPS	certificate practice statement
CRL	certificate revocation list
CTL	certificate trust list
EA	enrolment authority
EC	enrolment credential
ECIES	elliptic curve integrated encryption scheme
EE	end-entity (i.e. ITS trusted device)
GDPR	General Data Protection Regulation
HSM	hardware security module
ITD-POC	ITS data point of contact
PKI	public key infrastructure
RA	registration authority
SCMS	security credential management system
sub-CA	EA (enrolment authority) and AA (authorization authority)
TLM	trust list manager

4.3 Recommended abbreviated terms for security policy

The following abbreviated terms are not necessarily used in this document but are recommended for use when elaborating security policy. See Annex B.

CAM	cooperative awareness message
CP	certificate policy
DENM	decentralized environmental notification message
ISMS	information security management system
IVIM	infrastructure-to-vehicle information message
SCMS	security credential management system
SPATEM	signal phase and timing extended message
SREM	signal request extended message
SSEM	signal request status extended message

5 Summary of requirements in order to claim conformance with this document

5.1 General governance principles

See Annex A for information on the general context of governance principles. Note that informative Annex A contains no specific conformance requirements.

5.2 Conformance to this document (ISO 5616)

General conformance to this document may only be claimed if all of the requirements referenced in Clauses 5-9 are met.

A system may claim conformance to clearly identified specific parts of this document so long as that/those parts are clearly identified in the claim, and the claim is overtly and clearly restricted to those specific parts.

5.3 Permission of the owner of the data

Data access requires the permission of the owner of the data. Governance procedures at the application domain/service group level shall ensure that such permission is sought, and is provided freely, without duress or loss of other services if not given.

Any application that requires access to ITS data shall implement overt measures to request that the permission of the owner of the data to access and use that data is sought, and that such consent is provided freely, without duress, detriment or loss of other services if not given.

NOTE This requirement is as found in the GDPR in the European Union and similar data privacy and protection measures elsewhere.

The owners of an application shall provide evidence of their measures in this respect to the PMC (policy management committee). The RGMC (regional governance management committee) shall be asked to approve the PMC's means to do this.

5.4 Access to onboard data

Except where affected by national or regional regulations, conformance to the following existing documents is also required to enable consistent governance and operation of access to onboard data requirements as specified therein.

- ISO 15031-2, *Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 2: Guidance on terms, definitions, abbreviations and acronyms*;
- ISO 18541-1, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 1: General information and use case definition*;
- ISO 18541-2, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 2: Technical requirements*;
- ISO 18541-3, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 3: Functional user interface requirements*;
- ISO 18541-4, *Road vehicles — Standardized access to automotive repair and maintenance information (RMI) — Part 4: Conformance test*;
- ISO 20077-1, *Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information*;
- ISO 21177, *Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices* (see 5.5);
- ISO/TS 21184, *Cooperative intelligent transport systems (C-ITS) — Global transport data management (GTDM) framework* (see 5.6);

- ISO/TS 21185, *Intelligent transport systems — Communication profiles for secure connections between trusted devices* (see 5.7);
- ISO 21217, *Intelligent transport systems — Station and communication architecture;*
- ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary.*

5.5 Data available for full functional lifetime

Data made available shall be made available for the full functional lifetime of the entity providing the data, i.e. there shall be no arbitrary cut-off date. In the case of a software system or physical hardware, data shall be available until that system is formally decommissioned by its owner. In the case of a vehicle, data shall be until that vehicle is scrapped.

5.6 ITS data security and access

Regardless of the communications medium used to pass ITS data from one party to another, protocols and security shall conform to ISO 21177.

5.7 ITS data management

Regardless of the communications medium used to pass ITS data wirelessly from one party to another, data management and presentation shall conform to ISO/TS 21184.

5.8 ITS communications profiles

Regardless of the communications medium used to pass ITS data wirelessly from one party to another, protocols and security shall conform to ISO/TS 21185.

5.9 ITS communication media

The governance committee do not choose which wireless communications media are used (that is determined by the application domain/service group governance, or may be determined by legislation), but if a medium is selected, it needs to be used consistently across application domains using the same medium. Wired interfaces shall conform to normal wired communications and internet protocols.

While it is for the application domains/service groups to determine which communication media are appropriate for their application, they shall only adopt/select/use media for which there is a publicly available formally standardized (ISO/CEN/ETSI/ITU/UNECE, etc.) specification/standard that is suitable for use in combination with documents specified in 5.1 – 5.7.

While it is for the application domains/service groups to determine which communication media are appropriate for their application, they shall declare and submit their selection to the RGMC who shall inspect and ratify that it meets these criteria.

6 Governance method

6.1 The governance management committee (GMC) shall consider and approve or replace the techniques and protocols determined below at the earliest opportunity.

6.2 At the regional general management committee (RGMC) level, the chief executive shall monitor the operation of the systems using the secure interface and the operation of the security credential management system (SCMS), etc., and shall liaise with involved actors to identify and remedy any operational problems and issues.

6.3 The chief executive shall provide regular reports to the RGMC highlighting issues encountered in the operational measures of activities using the secure interface and the operation of the SCMS (security credential management system), etc., summarizing how the issue(s) have been addressed and reconciled. If any issues arise that cannot be reconciled, the chief executive shall report the issue to the RGMC, and, unless trivial, shall call a RGMC meeting to address the issue. At its discretion the RGMC may elevate an issue to the GMC through its chairperson.

6.4 On receiving the reports of the chief executive, if any regional governance committee member is not satisfied with the reconciliation of an issue, the regional governance committee member may request a meeting of the RGMC to discuss the issue and its reconciliation. If two or more regional governance committee members request such a RGMC meeting, the chief executive shall organize and hold such an RGMC meeting.

6.5 Similarly, at the international GMC level, if any governance committee member is not satisfied with the reconciliation of an issue, the governance committee member may request a meeting of the GMC to discuss the issue and its reconciliation.

7 Operation of the general management committee

7.1 For an overview of the architectural relationship between committees, see Figure 1.

7.2 It is anticipated that the GMC will elect a chairperson from its membership.

7.3 The GMC shall meet periodically, as appropriate, and shall determine international common protocols and practices.

NOTE The GMC can be an existing body such as UNECE WP1 or WP29 (and follow the existing "contracting party" agreements arrangements) or can be a body created for this specific purpose. An RGMC is likely to be organized to meet the needs of a region's political structure(s).

7.4 It is anticipated that the RGMC which has day to day issues to manage (such as certificate management, registries, etc.) shall appoint a chief executive officer (CEO), or equivalent management role. The means of financing the CEO and costs of operation of the RGMC shall be determined locally.

EXAMPLE The CEO can be a secondee of the regulator or an advertised position, or the whole task of managing the RGMC can be assigned to a commercial operation created by interested actors in the region, etc.

7.5 The chief executive should make, and be accountable for, day to day decisions.

7.6 The regulator representative and the C-ITS security credential management system (SCMS) shall be appointees of those organizations, but the other committee positions shall be open to challenge and appointment of the challenger or the re-election of the sitting member by the remainder of the RGMC. The Regulator shall, however, have a right to reject any candidate.

7.7 Regional governance principles shall take into consideration the regulations and the published policies of a regional authority (such as the European Commission, US DoT, NAFTA, Politbureau Standing Committee, etc.).

7.8 Governance policies shall, wherever possible, take into consideration standards and specifications approved by ballot of participating member states through a recognized standardization organization.

7.9 Only where standards and specifications approved by ballot of participating member states through a recognized standardization organization are not available can specifications and industry practices approved only by participating parties be considered and adopted. In this event, at the earliest opportunity, the approval of the use of the specification by ballot of participating member states through a recognized standardization organization shall be sought.

8 Procedures concerning “application domains” (e.g. service groups)

8.1 Procedures to establish a new application domain (e.g. service group)

The GMC and/or RGMC shall determine and make public the procedures to establish a new application domain (e.g. service group).

8.2 Roles and actors for each application domain/service grouping

8.2.1 General principles

The GMC and/or RGMC shall determine the expected actors for each application domain/service group, and the high-level roles for each actor, and shall seek participation from the identified actor groups to form the policy management committee (PMC) for that application domain/service group.

Qualification for membership and participation of a PMC shall initially be determined by the RGMC, and then reviewed between the RGMC and appointed members of the PMC, but shall generally fairly reflect the balance of the participants in the application domain. Once formed, the PMC shall review its membership from time to time and request the RGMC/GMC to add (or delete) representation of additional actors.

8.2.2 Example instantiation

An example of how this can be deployed in Europe is shown in Figure 2.

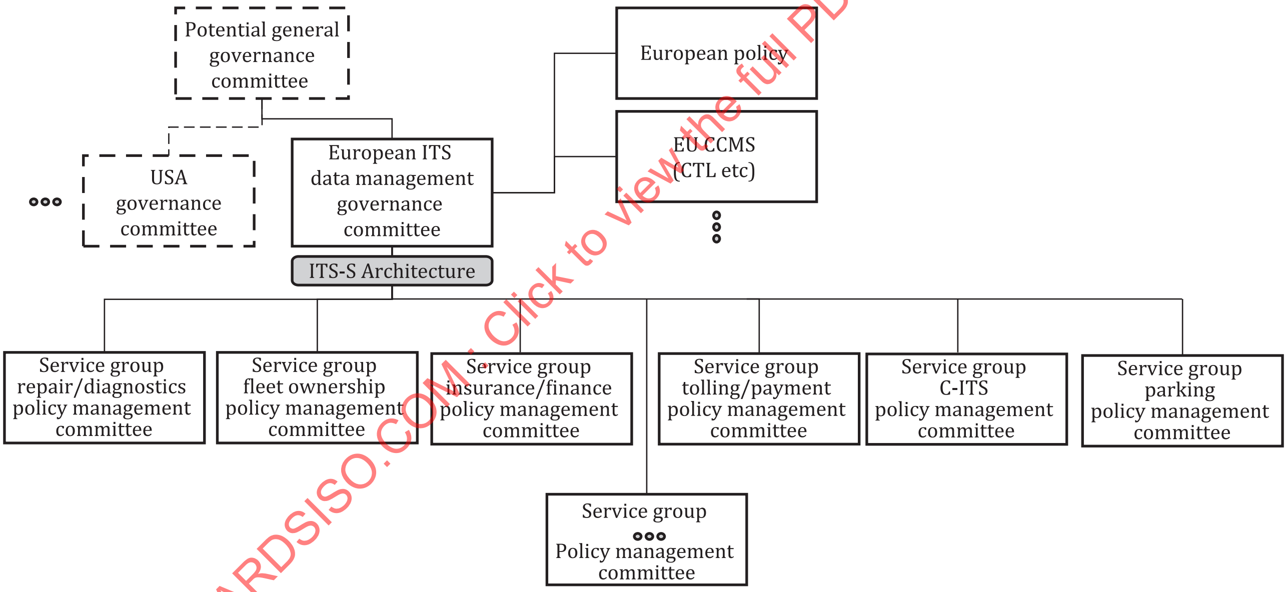

Potential general governance committee
European policy
EU CCMS (CTL etc)
USA governance committee
European ITS data management governance committee
ITS-S Architecture
Service group repair/diagnostics policy management committee
Service group fleet ownership policy management committee
Service group insurance/finance policy management committee
Service group tolling/payment policy management committee
Service group C-ITS policy management committee
Service group parking policy management committee
Service group ○○○ Policy management committee

Figure 2 — Example: possible instantiation in Europe

NOTE 1 This document does not choose/select which wireless (or wired) communications media are used. That is an operational decision.

NOTE 2 This document does not mandate any particular single communications media. For interoperability, it is recommended that secure wireless communications conform to one of a number of specified standards media, and conform to a nominated cybersecurity standard.

9 Application domain policy decision making

9.1 Context

ISO/TC 204 policy documents concerning ITS data governance policy have specified the governance framework for ITS data management and access, providing a generic description of the criteria for media, choice of media, and governance norms for cybersecurity, data presentation and data profiles (but excluding the selection/approval of media, which are operational /policy decisions). ISO/TC 204 policy documents also provide summary details of, or links to, publicly available government policy documents. Taken together, these provide an embracing paradigm for ITS data management and access, but they still present options which need policy decisions.

The current version of ISO/TC 204 policy documents concerning ITS data governance policy provides four different media options (more may follow in later editions). The originator and responder have to use a defined medium to originate the request for data and a defined medium to respond to the request. Request and response may often, but will not necessarily, use the same medium, and the same communication session, but in all cases the medium used to request shall be defined, and in all cases the medium used to respond shall be defined. These are decisions to be made jointly between the RGMC and the appropriate user community.

Policies need to be consistent with, and operate within the governance specifications defined herein, but the detail of the policies will be different in different scenarios (for example, C-ITS safety messages will differ from policies for access to on-board data for maintenance and repair, or from usage-based insurance, or for fleet management/rental fleet management). Thus, the user community has to determine its exact policies and choices and access rights. This is achieved through a policy management committee (PMC) for the application domain (e.g. service group).

Policies and protocols are required to be licit. As such, once determined by the user community, they have to be submitted to, and ratified by, the RGMC/GMC.

Each application domain/service group shall define the policies and protocols for their constituency, and submit this for ratification with the RGMC.

Annex B provides guidance/pro forma/checklist templates to assist user communities in determining their exact policies and choices.

Each application domain/service group shall determine and publish who sits on the committee, and normal governance/management for this group, subject to the approval of the RGMC.

Each application domain/service group shall develop/provide an application domain description, including which standards and regulations are involved.

Each application domain/service group shall determine and publish which data and functions are needed, and who needs access to which specific data and under which conditions.

Each application domain/service group shall determine and publish how security functions shall be implemented (which certificates are needed, who obtains them, under which conditions).

In respect of the governance of ITS trusted devices, it is recommended that this aspect has a separate ITS station governance committee for each RGMC, that shall determine features for the entire ITS station as a platform:

- communications, memory size, other technical parameters;
- security provisions on a station level;
- ITS station manager for full life cycle QA of ITS-S;
- who is required to have an ITS-S from the start, and how to approve after-market equipping.

9.2 Determination of policy

9.2.1 Policy making requirements

An RGMC (individually or in concert with the GMC), having identified a use-case requirement, shall establish a representative committee of interested experts [the policy management committee (PMC)] to propose a policy document for the identified use-case(s). Policies, once agreed, will be sent to the RGMC/GMC for ratification, and then published.

The representative committee of interested experts (PMC) shall comprise representation from the RGMC, GMC (where multiple RGMCs are involved), and stakeholder organizations such as industry associations, certificate authorities, commercial service providers, other actors from the application domain (e.g. service group).

The PMC for each application domain/service group shall define the operational requirements, processes and protocol for their constituency and provide specification, such as those listed below.

9.2.2 High level operational process description

The PMC shall develop and publish its operational practice(s) and protocols for access to data. These will vary according to the use-case(s) supported by the PMC, but shall include:

a) eligibility/qualifying criteria;

b) use-cases supported;

c) terms of access;

d) registration process;

e) service provided by PMC;

f) fees charged by PMC;

g) any other fees.

9.2.3 Defining operational model and bylaws

The PMC shall develop and publish its operational model and bylaws:

- structure and management;
- financing/business model;
- a service description;
- revue and decision regarding available options provided by GMC/RGMC;
- standards accepted and adopted (in addition to GMC/RGMC requirements);
- ITS station governance regarding features for the entire ITS station as a platform;
- service(s) definition and extent of scope;
- specify application and components;
- aftermarket aspects where appropriate;
- management policies for whole system lifecycle.

9.2.4 Access controls

9.2.4.1 Parties/devices accessing ITS/vehicle data shall be authenticated before access can be granted:

- authentication protocol definition.

9.2.4.2 Secure access to ITS/vehicle data requires the use of digital certificates. Connected devices require digital certificates. Backend servers also require digital certificates. Access is controlled through configuration files based on use case requirements (e.g. an insurer's data needs are different to those of a diagnostic technician):

- definition of access conditions, routines and protocols (consistent with GMC/RGMC principles).

9.2.5 Election and ejection criteria and procedures

This subclause provides a list of aspects to be considered and specified/determined by the RGMC and/or PMC:

a) who can provide service and to whom;

b) characteristics of the service provider;

c) characteristics of service recipient;

d) how to approve after-market fitting (where appropriate).

9.2.6 Data and actions required

This subclause provides a non-exhaustive list of aspects to be considered and specified/determined by the RGMC and/or PMC:

a) GDPR/regional privacy regulations;

b) levels of security requirements;

c) certificate issuing procedures;

d) lifetime definition;

e) revocation procedures;

f) testing, approval, rejection/recall procedures;

g) what data and functions are needed, and who needs access under what conditions.

9.2.7 Policy examples

As stated in 9.1, the user community is required to determine its exact policies and choices.

Annex B provides guidance/pro forma/checklist templates to assist user communities in determining their exact policies and choices.

Annex A
(informative)

Principles of governance

A.1 Overview

This annex specifies the general principles of governance on which this document is based.

A.2 What is Governance?

A definition of the term “governance” is provided in term 3.1.5.

A.3 Collaborative governance

Governance is a broader concept than government, and also includes the roles played by the community sector and the private sector in managing and planning countries, regions and cities. Collaborative governance involves the government, community and private sectors communicating with each other and working together to achieve more than any one sector could achieve on its own.

Collaborative governance covers both the informal and formal relationships in problem solving and decision-making. Conventional government policy processes can be embedded in wider policy processes by facilitating collaboration between the public, private and community sectors.

Collaborative governance requires three things, namely:

— support;

— leadership; and

— a forum.

The support function identifies the policy problem to be fixed.

The leadership function gathers the sectors into a forum.

Then, the members of the forum collaborate to develop policies, solutions and answers.

A.4 ICT governance

Information technology (IT) governance is a subset discipline of corporate governance, focused on IT and its performance and risk management.

IT governance systematically involves everyone: board members, executive management, staff, customers, communities, investors and regulators.

Information and communications technology (ICT) is a term that stresses the role of unified communications and the integration of telecommunications and computers, as well as systems that enable users to access, store, transmit and manipulate information.

In addition to IT governance issues, ICT introduces the governance of the communication issues as well. This introduces issues such as communication access, communication costs, interference, cybersecurity, cybercrime and cyberwar. Data access and ownership is primarily an IT issue, but is complicated by communications accessibility issues, and complicated further by the GDPR in the European Union [see, for example, the certificate policy of the European C-ITS “trust model” based on public key infrastructure (PKI) within the scope of the overall EU C-ITS security credential management system (EU CCMS)], and similar privacy/data protection legislation in other regions.

Rapid changes in information and communication technologies mean that ensuring the security of communication networks presents a singular challenge, and need to be governed and actively managed. Issues of migration and migratability need to be governed from the outset.

Regulatory processes offer one route to manage these processes, however, the regulatory process is invariably exceedingly slow and inflexible, especially for rapidly evolving technologies. It is also often marred by political compromises. Network security agreements can offer more flexible alternatives.

A.5 Governance model/ governance plan

Within the agreed governance model, a “governance plan” refers to roles and processes in an enterprise that serve as a guideline for fulfilling, sustaining and extending the service planning.

A governance plan crosses all organizational layers, including stakeholders, administration, maintenance, strategy, policy and support

A.6 Multistakeholder governance model

Multistakeholder governance are new and evolving governance systems that attempt to embrace the complexities of the modern connected world. Historically a government governed by statute and regulation; a utility operated within that paradigm governed by a management board to some type of charter; and commercial organizations were/are governed by a board of directors appointed by shareholders. Each governed on a day-to-day level, largely discretely.

Thus the government would provide the road infrastructure and rules of the road determined by politicians, and would manage and police the road network; fuel and public transport would be provided by a utility organization in some cases, and in other cases by large commercial organizations, or a mixture of both; and vehicles would be made by automotive manufacturers, each actor group implementing aspects that interoperate, but largely governing themselves discretely.

The modern connected paradigm changes that archetype such that each of the actors not only interoperates with other actors, but is reliant and interdepends on the other actors, such that it can no longer achieve/perform its function on a day to day, minute-by-minute, possibly even second-by-second, basis, without that interaction/interdependence.

Today, and particularly in the transport sector, actors cannot provide their function without increasingly connected interoperation, particularly in a CCAM paradigm that considers “journeys” above particular modes of transport; where vehicles need to talk to each other and communicate with the infrastructure; and, particularly with the rapidly approaching onset of connected (driver assistance systems)/automated driving.

In this paradigm, discrete independent governance provides only incompatibility and service failure.

Not everything, but the interdependent aspects, require multistakeholder governance in order to succeed. Multistakeholder governance seeks to bring stakeholders together to participate in the dialogue, decision making, and implementation of responses to jointly perceived paradigms and their associated issues and problems.

“Stakeholders”, in this case, refers to a collection of actors from different social, political and economic spheres, working intentionally together to govern a physical, social, economic or policy paradigm (i.e. to provide governance of an agreed domain within which theories, laws and generalizations and the experiments performed in support of them are formulated).

A.7 Nine stages of an effective governance model/process (referenced to its data access and management)

1) Identify the subject that is to be governed.

2) Identify the key actors involved in the subject that is to be governed.

3) Identify the key actors involved in the governance process.

4) Define your global goals and objectives. (The first step/milestone in designing a governance process is to determine what the goals are for your governed domain).

5) Evaluate your resources.

6) Plan your processes.

7) (S)elect governance lead.

8) Create scalable documentation and processes.

9) Train your team and internal clients.

A.8 Key attributes of certificate policy

A.8.1 Overview

The following attributes are common features of certificate policy implementation and common understanding and use is recommended when elaborating certificate policy.

NOTE The following attributes are described for guidance and are not defined requirements of this document.

A.8.2 Applicant

A natural person or legal entity that applies for (or seeks renewal of) a certificate is commonly known as an applicant. Once the initial certificate is created (initialisation), the applicant is then commonly referred to as the subscriber.

NOTE For certificates issued to end-entities, the subscriber (certificate applicant) is the entity that controls or operates/maintains the end-entity to which the certificate is issued, even if the end-entity is sending the actual certificate request.

A.8.3 Authorization authority

The specific function of the authorization authority (AA), and also the legal and/or operational entity managing it, are generically described as the authorization authority.

A.8.4 Certification authority

The root certification authority, enrolment authority and authorization authority are cumulatively referred to as the certification authority (CA).

A.8.5 Crypto-agility

The capability of the ITS-data “trust model” entities to adapt the certificate policy to changing environments or to new future requirements (e.g. by a change of cryptographic algorithms and key length over time) is generally described as crypto-agility.

A.8.6 Cryptographic module

A secure hardware-based element within which keys are generated and/or stored, random numbers are generated and data are signed or encrypted is known as a cryptographic module.

A.8.7 Enrolment authority

An authority in the ITS PKI (public key infrastructure) structure that authenticates an ITS-S (ITS-station) and grants it access to ITS communication (which may be made pseudonymous by authorizing access to relevant authorization authority/ies) to grant authorization for specific services is known as an enrolment authority.

A.8.8 ITS-data trust model

The model responsible for establishing a relationship of trust between ITS trusted devices is generally known as a data-trust model (in this use-case, the ITS-data trust model).

NOTE It is typically implemented through the use of a PKI (public key infrastructure) composed of root CAs (certification authorities), the ITD-POC (ITS data point of contact), TLM (trust list manager), EAs (enrolment authority), AAs (authorization authorities) and a secure network.

A.8.9 PKI participants

Entities of the ITS-data "trust model", i.e. the TLM (trust list manager), root CAs (certification authorities), EAs (enrolment authorities), AAs (authorization authorities) and C-ITS stations are generically described as PKI participants.

A.8.10 Re-keying

The subcomponent activity used to describe certain elements relating to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key is known as re-keying.

A.8.11 Repository

The entity used for storing the certificates and information on certificates provided by the entities of the ITS-data "trust model" is generally known as a repository.

A.8.12 Root certification authority

The specific function of the CA (certification authority) combined with the legal and/or operational entity managing it is known as the root certification authority.

A.8.13 Subject

A natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber, is known as the subject.

A.8.14 Subscriber

A natural person or legal entity to which a certificate is issued and that is legally bound by a terms of use agreement is known as a subscriber.

A.8.15 Subscriber agreement

An agreement between the CA (certification authority) and the applicant/subscriber that specifies the rights and responsibilities of the parties is known as a subscriber agreement.

A.9 Key attributes of security policy

A.9.1 Overview

The following attributes are common features of security policy implementation and common understanding and use is recommended when elaborating security policy.

NOTE The following attributes are described for guidance and are not defined requirements of this document.

A.9.2 Availability

Availability is a term used to describe the condition of being accessible and usable on demand by an authorized entity (see ISO/IEC 27000).

A.9.3 Confidential information

Information that is not to be made available or disclosed to unauthorized individuals, entities or processes is generally described as confidential information (see ISO/IEC 27000).

A.9.4 Information security

Information security is the term commonly used for aspects concerning the preservation of the confidentiality, integrity and availability of information (see ISO/IEC 27000).

A.9.5 Information security incident

An unwanted or unexpected information security event, or series of events, that has a significant probability of compromising business operations and threatening information security is generally known as an information security incident.

A.9.6 Integrity

The property of accuracy and completeness of data or information is described as its integrity (ISO/IEC 27000).

A.9.7 ITS trusted device infrastructure

The system of facilities, equipment and applications needed for the operation of an organization that provides ITS trusted device services related to fixed ITS trusted devices is generally known as the ITS trusted device infrastructure.

A.9.8 ITS trusted device stakeholders

Individuals, groups or organizations with a role and responsibility in the ITS trusted device network are generally known as ITS trusted device stakeholders.

A.9.9 Local dynamic map (LDM)

An in-vehicle ITS trusted device station's dynamically updated repository of data relating to local driving conditions is generally known as a local dynamic map. It includes information received from on-board sensors and from CAM and DENM messages (see ETSI TR 102 893).[3]

A.9.10 Protocol control

Protocol control is the term generally used to describe the use of assets which select an appropriate message transfer protocol for an outgoing message request and send the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the ITS trusted device and passed to the relevant functional asset for further processing (see ETSI TR 102 893).

Annex B
(informative)

Pro forma tables of contents and templates

B.1 Certificate policy

B.1.1 Recommended table of contents for certificate policy

The following lists are elaborated to be generally useful and informative as an aide/guide to aspects to be considered by RGMCs when determining/developing their certificate policy. It is not intended as a mandatory set of requirements.

1. Introduction

1.1. Overview and scope of this policy

1.2. Definitions and acronyms

1.3. PKI participants *Description/Definition*

1.3.1. Introduction

1.3.2. ITS trusted device certificate policy authority

1.3.3. Trust list manager

1.3.4. Accredited public key infrastructure (PKI) auditor

1.3.5. ITS trusted device point of contact (ITD-POC)

1.3.6. Operational roles

1.4. Certificate usage. *Description/Definition*

1.4.1. Applicable domains of use

1.4.2. Limits of responsibility

1.5. Certificate policy administration *Procedures*

1.5.1. Updating of CPSs (certificate practice statements) of CAs (certification authorities) listed in the regional certificate trust list (CTL)

1.5.2. CPS (certificate practice statement) approval procedures

2. Publication and repository responsibilities *Description/Definition/Procedures*

2.1. Methods for the publication of certificates information

2.2. Time or frequency of publication

2.3. Repositories

2.4. Access controls on repositories

2.5. Publication of certificate information

2.5.1. Publication of certificate information by the TLM (trust list manager)

2.7.2. Publication of certificate information by CAs (certification authorities)

3. Identification and authentication *Definition*

3.1. Naming

3.1.1. Types of name

3.1.1.1. Names for TLM (trust list manager), root CAs (certification authorities), EAs (enrolment authorities), AAs (authorization authorities)

3.1.1.2. Names for end-entities

3.1.1.3. Identification of certificates

3.1.2. Need for names to be meaningful

3.1.3. Anonymity and pseudonymity of end-entities

3.1.4. Rules for interpreting various name forms

3.1.5. Uniqueness of names

3.2. Initial identity validation *Procedures*

3.2.1. Method to prove possession of private key

3.2.2. Authentication of organization identity

3.2.2.1. Authentication of root CAs (certification authorities) organization identity

3.2.2.2. Authentication of TLM (trust list manager) organization identity

3.2.2.3. Authentication of sub-CAs organization identity

3.2.2.4. Authentication of end-entities subscriber organization

3.2.3. Authentication of individual entity *Procedures*

3.2.3.1. Authentication of TLM (trust list manager)/CA individual entity

3.2.3.2. Authentication of ITS trusted device subscriber identity

3.2.3.3. Authentication of ITS trusted device identity

3.2.4. Non-verified subscriber information

3.2.5. Validation of authority *Procedures*

3.2.5.1. Validation of TLM (trust list manager), root CA (certification authority), EA (enrolment authority), AA (authorization authority)

3.2.7.2. Validation of ITS trusted device subscribers

3.2.5.3. Validation of ITS trusted device

3.2.6. Criteria for interoperation *Procedures*

3.3. Identification and authentication for re-key requests *Procedures*

3.3.1 Identification and authentication for routine re-key requests

3.3.1.1. TLM (trust list manager) certificates

3.3.1.2. Root CA (certification authority) certificates

3.3.1.3. EA (enrolment authority)/AA (authorization authority) certificate renewal or re-keying

3.3.1.4. End-entities enrolment credentials

3.3.1.5. End-entities authorization tickets

3.3.2. Identification and authentication for re-key requests after revocation

3.3.2.1. CA (certification authority) certificates

3.3.2.2. End-entities enrolment credentials

3.3.2.3. End-entities authorization requests

3.4. Identification and authentication for revocation request

3.4.1. Root CA (certification authority)/EA (enrolment authority) and AA (authorization authority) certificates

3.4.2. ITS trusted device enrolment credentials

3.4.3. ITS trusted device authorization tickets

4. Certificate Life-cycle operational requirements *Definition/Procedures*

4.1. Certificate application

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

4.2.1.1. Identification and authentication of root CAs (certification authorities)

4.2.1.2. Identification and authentication of the TLM (trust list manager)

4.2.1.3. Identification and authentication of EA (enrolment authority) and AA (authorization authority)

4.2.1.4. Identification and authentication of EE subscriber

4.2.1.5. Authorization tickets

4.2.2. Approval or rejection of certificate applications

4.2.2.1. Approval or rejection of root CA (certification authority) certificates

4.2.2.2. Approval or rejection of TLM (trust list manager) certificate

4.2.2.3. Approval or rejection of EA (enrolment authority) and AA (authorization authority) certificates

4.2.2.4. Approval or rejection of enrolment credential

4.2.2.5. Approval or rejection of AT (authorization ticket)

4.2.3. Time to process the certificate application

4.2.3.1. Root CA (certification authority) certificate application

4.2.3.2. TLM (trust list manager) certificate application

4.2.3.3. EA (enrolment authority) and AA (authorization authority) certificate application

4.2.3.4. Enrolment credential application

4.2.3.5. AT (authorization ticket) application

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

4.3.1.1. Root CA (certification authority) certificate issuance

4.3.1.2. TLM (trust list manager) certificate issuance

4.3.1.3. EA (enrolment authority) and AA (authorization authority) certificate issuance

4.3.1.4. Enrolment credential issuance

4.3.1.5. AT (authorization ticket) issuance

4.3.2. CA's notification to subscriber of issuance of certificates

4.4. Certificate acceptance

4.4.1. Conducting certificate acceptance

4.4.1.1. Root CA (certification authority)

4.4.1.2. TLM (trust list manager)

4.4.1.3. EA (enrolment authority) and AA (authorization authority)

4.4.1.4. ITS trusted device

4.4.2. Publication of the certificate

4.4.3. Notification of certificate issuance

4.5. Key pair and certificate usage

4.5.1. Private key and certificate usage

4.5.1.1. Private key and certificate usage for TLM (trust list manager)

4.5.1.2. Private key and certificates usage for root CAs (certification authorities)

4.5.1.3. Private key and certificate usage for EAs (enrolment authorities) and AAs (authorization authority)

4.5.1.4. Private key and certificate usage for end-entity

4.7.2. Relying party public key and certificate usage

4.6. Certificate renewal *Definition/Procedures*

4.7. Certificate re-key *Definition/Procedures*

4.7.1. Circumstances for certificate re-key

4.7.2. Who may request re-key

4.7.2.1. Root CA (certification authority)

4.7.2.2. TLM (trust list manager)

4.7.2.3. EA (enrolment authority) and AA (authorization authority)

4.7.2.4. ITS trusted device

4.7.3. Re-keying process

4.7.3.1. TLM (trust list manager) certificate

4.7.3.2. Root CA (certification authority) certificate

4.7.3.3. EA (enrolment authority) and AA (authorization authority) certificates

4.7.3.4. ITS trusted device certificates

4.8. Certificate modification *Definition/Procedures*

4.9. Certificate revocation and suspension *Definition/Procedures*

4.10. Certificate status services *Definition/Procedures*

4.10.1. Operational characteristics

4.10.2. Service availability

4.10.3. Optional features

4.11. End of subscription *Definition/Procedures*

4.12. Key escrow and recovery *Definition*

4.12.1. Subscriber

4.12.1.1. Which key pair can be escrowed

4.12.1.2. Who can submit a recovery application

4.12.1.3. Recovery process and responsibilities

4.12.1.4. Identification and authentication

4.12.1.5. Approval or rejection of recovery applications

4.12.1.6. KEA and KRA actions during key pair recovery

4.12.1.7. KEA and KRA availability

4.12.2. Session key encapsulation and recovery policy and practices

5. Facility, management and operational controls *Definition/Procedures*

5.1. Physical controls

5.1.1. Site location and construction

5.1.1.1. Root CA (certification authority), CPOC (C-ITS Point of Contact) , TLM (trust list manager)

5.1.1.2. EA (enrolment authority) / AA (authorization authority)

5.1.2. Physical access

5.1.2.1. Root CA (certification authority), CPOC, TLM (trust list manager)

5.1.2.2. EA (enrolment authority) and AA (authorization authority)

5.1.3. Power and air conditioning

5.1.4. Water exposures

5.1.5. Fire prevention and protection

5.1.6. Media management

5.1.7. Waste disposal .

5.1.8. Off-site backup

5.1.8.1. Root CA (certification authority), CPOC and TLM (trust list manager)

5.1.8.2. EA (enrolment authority) and AA (authorization authority)

5.2. Procedural controls

5.2.1. Trusted roles

5.2.2. Number of persons required per task

5.2.3. Identification and authentication for each role

5.2.4. Roles requiring separation of duties

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements

5.3.2. Background check procedures

5.3.3. Training requirements

5.3.4. Retraining frequency and requirements

5.3.5. Job rotation frequency and sequence

5.3.6. Sanctions for unauthorized actions

5.3.7. Independent contractor requirements

5.3.8. Documentation supplied to personnel

5.4. Audit logging procedures

5.4.1. Types of event to be recorded and reported by each CA (certification authority)

5.4.2. Frequency of processing log

5.4.3. Retention period for audit log

5.4.4. Protection of audit log

5.4.5. Audit log backup procedures

5.4.6. Audit collection system (internal or external)

5.4.7. Notification to event-causing subject

5.4.8. Vulnerability assessment

5.5. Record archiving

5.5.1. Types of record archived

5.7.2. Retention period for archive

5.5.3. Protection of archive

5.5.4. System archive and storage

5.5.5. Requirements for time-stamping of records

5.5.6. Archive collection system (internal or external)

5.5.7. Procedures to obtain and verify archive information

5.6. Key changeover for ITS trusted device “trust model” elements

5.6.1. TLM (trust list manager)

5.6.2. Root CA (certification authority)

5.6.3. EA (enrolment authority) and AA (authorization authority) certificate

5.6.4. Auditor

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling

5.7.2. Corruption of computing resources, software and/or data

5.7.3. Entity private key compromise procedures

5.7.4. Business continuity capabilities after a disaster

5.8. Termination and transfer

5.8.1. TLM (trust list manager)

5.8.2. Root CA (certification authority)

5.8.3. EA (enrolment authority)

6 Generation and installation

6.1. Key-pair generation and installation

6.1.1. TLM (trust list manager), root CA (certification authority), EA (enrolment authority), AA (authorization authority)

6.1.2. EE (end-entity) — mobile ITS trusted device

6.1.3. EE (end-entity) — fixed ITS trusted device

6.1.4. Cryptographic requirements

6.1.4.1. Algorithm and key length — signature algorithms

6.1.4.2. Algorithm and key length — encryption algorithms for enrolment and authorization

6.1.4.3. Crypto-agility

6.1.5. Secure storing of private keys

6.1.5.1. Root CA (certification authority), sub-CA and TLM (trust list manager) level

6.1.7.2. End-entity

6.1.6. Backup of private keys

6.1.7. Destruction of private keys

6.2. Activation data

6.3. Computer security controls

6.4. Life-cycle technical controls

6.5. Network security controls

7. Certificate profiles, CRL (certificate revocation list) and CTL (certificate trust list) *Definition/Procedures*

7.1. Certificate profile

7.2. Certificate validity

7.2.1. Pseudonym certificates

7.2.2. Authorization tickets for fixed ITS trusted device stations

7.3. Revocation of certificates

7.3.1. Revocation of CA (certification authority), EA (enrolment authority) and AA (authorization authority) certificates

7.3.2. Revocation of enrolment credentials

7.3.3. Revocation of authorization tickets

7.4. Certificate revocation list

7.5. European certificate trust list

8. Compliance audit and other assessments *Definition/Procedures*

8.1. Topics covered by audit and audit basis

8.2. Frequency of the audits

8.3. Identity/qualifications of auditor

8.4. Auditor's relationship to audited entity

8.5. Action taken as a result of deficiency

8.6. Communication of results

9. Other provisions *Definition*

9.1. Fees

9.2. Financial responsibility

9.3. Confidentiality of business information

9.4. Privacy plan

10. References

B.1.2 Recommended definitions for certificate policy

It is preferable to use common definitions of terms used in the discussion/implementation of certificate policy. A list of recommended common definitions for certificate policy is provided in 3.2.

B.1.3 Recommended abbreviated terms for certificate policy

It is preferable to use common abbreviations of terms used in the discussion/implementation of certificate policy. A list of recommended common abbreviated terms for certificate policy is provided in 4.2.

B.1.4 Generic Figures and diagrams for certificate policy

The following figures and diagrams provide examples to assist the reader in understanding the context and aspects involved in certificate policy.

NOTE These are examples to assist comprehension and are not specified requirements.

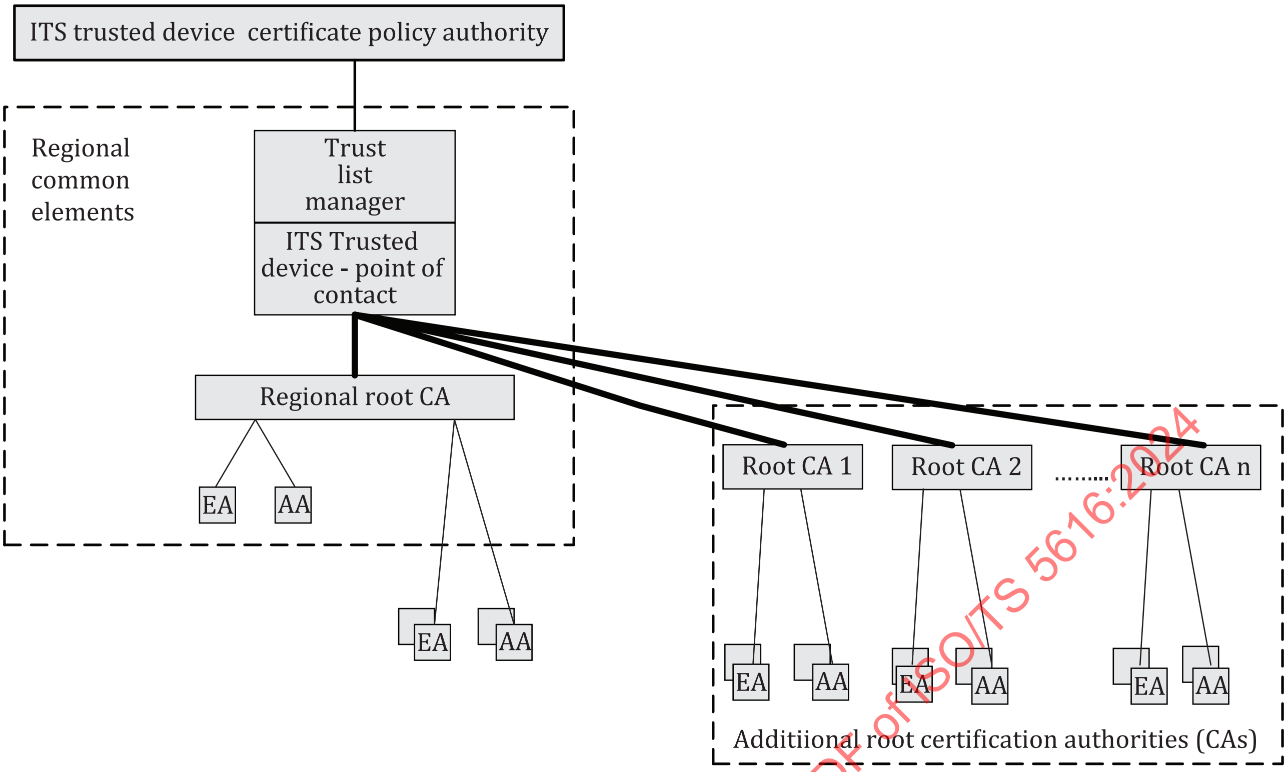
Figure B.1 shows an example of the interrelationships involved in a certificate policy trust model.

Figure B.2 provides a high-level example of the information flows involved in a certificate policy trust model.

Table B.1 provides an example of the more detailed typical transactional information flows involved in a certificate policy trust model.

Table B.2 provides an example of the operational roles involved in a certificate policy trust model.

Table B.3 provides an example of the re-keying processes involved in a certificate policy trust model.


ITS trusted device certificate policy authority
Regional common elements
Trust list manager
ITS Trusted device - point of contact
Regional root CA
EA
AA
EA
AA
Root CA 1
Root CA 2
Root CA n
EA
AA
EA
AA
EA
AA
Additiional root certification authorities (CAs)

Key

EA	enrolment authority
AA	authorization authority
CA	certification authority
▬	trust relation

Figure B.1 — ITS trusted device: example "trust model" architecture

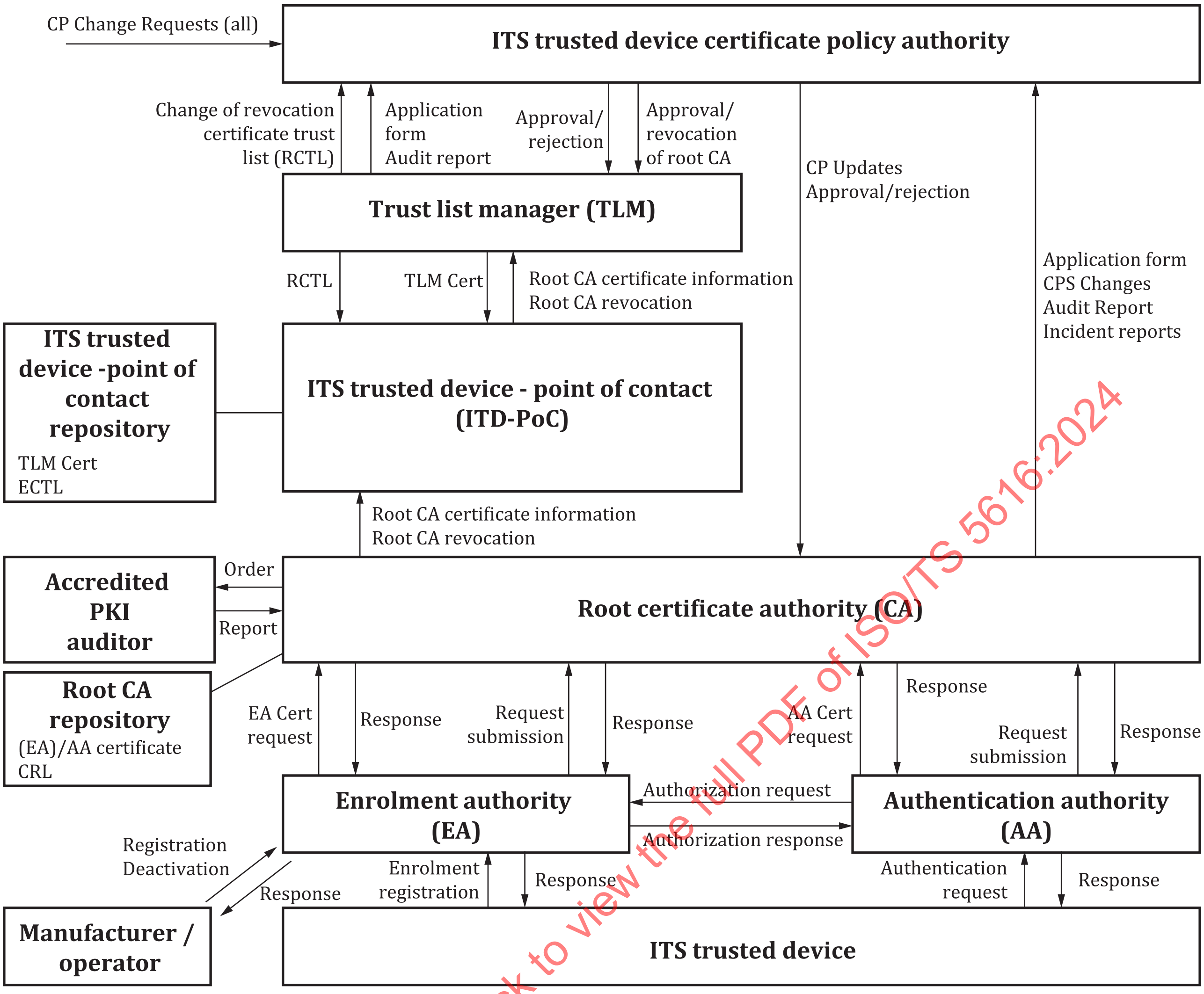


Figure B.2 — ITS trusted device: example “trust model” information flows

Table B.1 — Detailed description of information flows in the ITS trusted device “trust model”

Flow ID	From	To	Content
(1)	CPA (certificate policy authority)	TLM (trust list manager)	approval of root CA (certification authority) application
(2)	CPA (certificate policy authority)	TLM (trust list manager)	information on revocation of root CA (certification authority)
(3)	CPA (certificate policy authority)	root CA (certification authority)	CP updates
(4)	CPA (certificate policy authority)	root CA (certification authority)	approval/rejection of root CA (certification authority) application form or the CPS (certificate practice statement), request changes to the audit process.
(5)	TLM (trust list manager)	CPA (certificate policy authority)	notification of change of RCTL
(6)	TLM (trust list manager)	ITD-POC	TLM certificate
(7)	TLM (trust list manager)	ITD-POC	RCTL
(8)	CPOC	TLM (trust list manager)	root CA (certification authority) certificate information