Technical Specification

ISO/TS 5616

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

First edition
2024-12

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

Page

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.

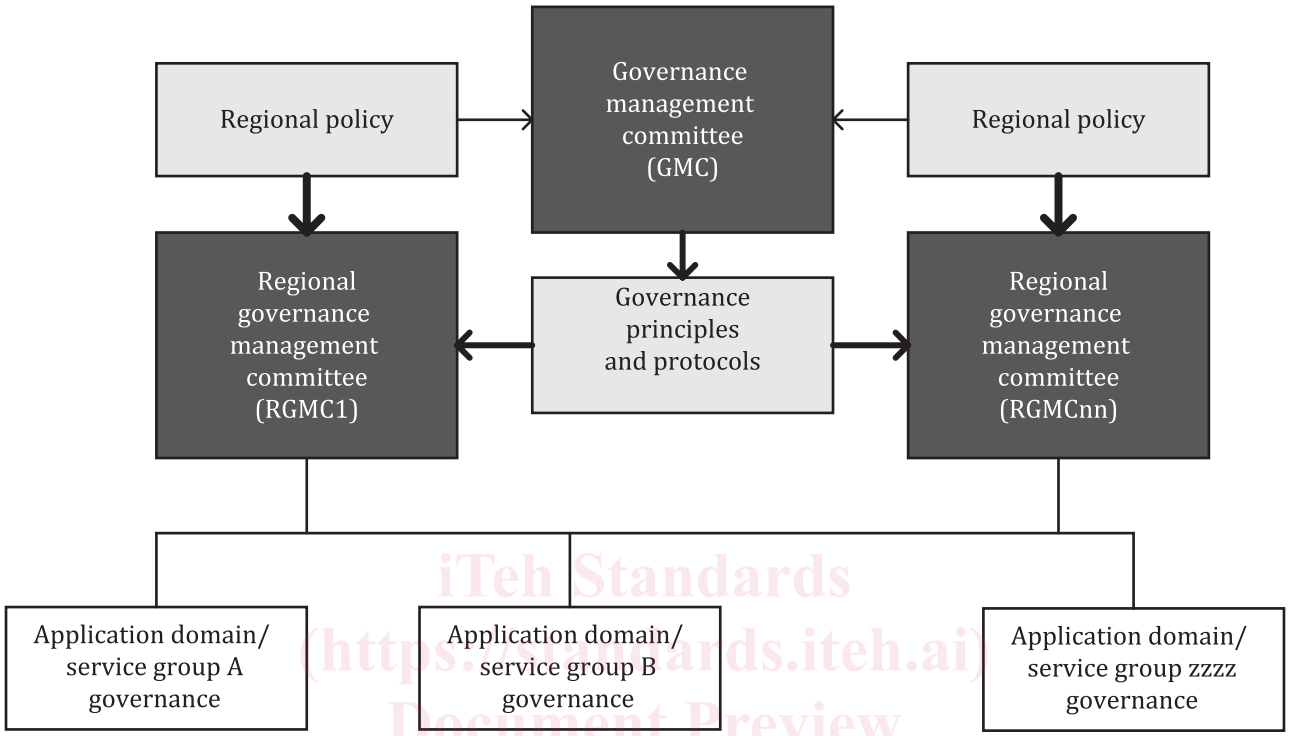

Figure 1 — Conceptual governance reference architecture

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.