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 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
3.1 General terms used in this document ... 2
3.2 Recommended definitions for certificate policy (Annex A) ... 4
3.3 Recommended definitions for security policy (Annex A) ... 5
4 Abbreviated terms ... **6**
4.1 General abbreviated terms used in this document ... 6
4.2 Recommended abbreviated terms for certificate policy ... 6
4.3 Recommended abbreviated terms for security policy ... 7
5 Summary of requirements in order to claim conformance with this document ... **8**
5.1 General governance principles ... 8
5.2 Conformance to this document (ISO 5616) ... 8
5.3 Permission of the owner of the data ... 8
5.4 Access to onboard data ... 8
5.5 Data available for full functional lifetime ... 9
5.6 ITS data security and access ... 9
5.7 ITS data management ... 9
5.8 ITS communications profiles ... 9
5.9 ITS communication media ... 9
6 Governance method ... **9**
7 Operation of the general management committee ... **10**
8 Procedures concerning "application domains" (e.g. service groups) ... **11**
8.1 Procedures to establish a new application domain (e.g. service group) ... 11
8.2 Roles and actors for each application domain/service grouping ... 11
8.2.1 General principles ... 11
8.2.2 Example instantiation ... 11
9 Application domain policy decision making ... **12**
9.1 Context ... 12
9.2 Determination of policy ... 13
9.2.1 Policy making requirements ... 13
9.2.2 High level operational process description ... 13
9.2.3 Defining operational model and bylaws ... 13
9.2.4 Access controls ... 14
9.2.5 Election and ejection criteria and procedures ... 14
9.2.6 Data and actions required ... 14
9.2.7 Policy examples ... 14
Annex A (informative) **Principles of governance** ... **15**
Annex B (informative) **Pro forma tables of contents and templates** ... **20**
Bibliography ... **38**

© ISO 2024 – All rights reserved

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.

© ISO 2024 – All rights reserved

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.

© ISO 2024 – All rights reserved

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.

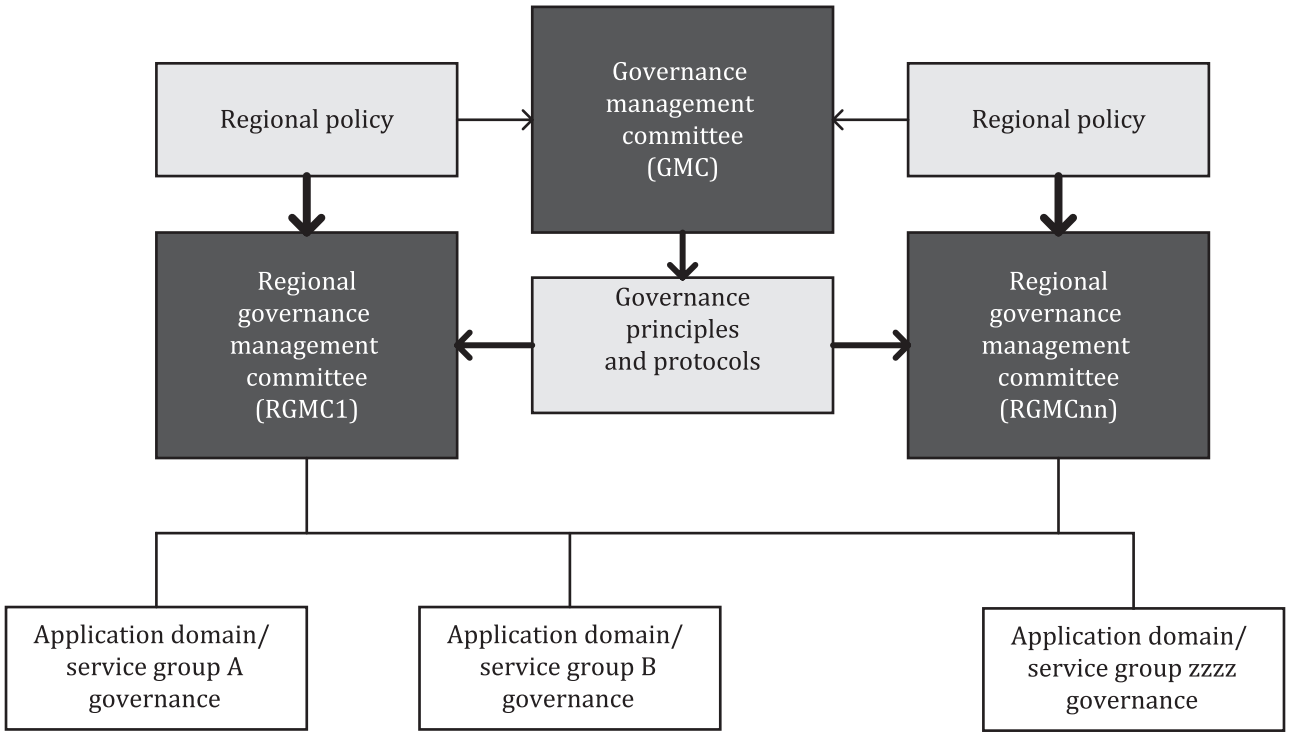


Figure 1 — Conceptual governance reference architecture

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.

© ISO 2024 – All rights reserved

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*

© ISO 2024 – All rights reserved