ISO/DISPRF 15784-2:2023(E)

ISO-<u>/</u>TC-<u>2</u>04/WG 9

Date: 2024-01-09

Secretariat: ANSI

Date: 2024-04-17

Intelligent transport systems—— Data exchange involving roadside modules communication—_

Part-_2: Centre to field device communications using Simple Network **Management Protocol (SNMP)**

Systèmes intelligents de transport (SIT) — Échange de données impliquant la communication de modules en <u>bordure de route —</u>

<u>Partie 2: Communications par dispositif du centre au terrain en utilisant le protocole simple de gestion de</u> réseau (SNMP)

PROOF

© 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 EmailE-mail: copyright@iso.org Website: www.iso.orgwww.iso.org

Published in Switzerland

iTeh Standards (https://standards.iteh.ai) Document Preview

ISO/PRF 15784-2

https://standards.jteh.aj/catalog/standards/jso/f8554c43-c751-4caa-b689-efef867e2d98/jso-prf-15784-2

© ISO 2023 - All rights reserved

ii

Contents Page

Forew	<u>ordvi</u>
Introd	uctionvii
1	<u>Scope</u> 1
2	Normative references2
3	Terms and definitions
4	Abbreviated terms4
<u>5</u>	Conformance and Conventions5
5.1	ASN.1
5.2	SNMP Terminology
5.3	Format 5
5.4	Conformance5
6	Architecture6
6.1	ITS services 6
6.2	Physical view6
6.3	Communications view
7	Requirements9
<u>7.1</u>	Overview9
7.2	Terminology and internal architecture10
7.3	Message Processing and Dispatching10
7.4	Applications10
<u>7.4.1</u>	
<u>7.4.2</u>	Command generator10
7.4.3	Command responder10
<u>7.4.4</u>	<u>Notification originator</u> 11
<u>7.4.5</u>	Notification receiver11
<u>7.4.6</u>	
7.5	Security models11
7.5.1	User-based security model11
7.5.2	Transport security model 12
<u>7.6</u>	View-based access control
7.7	Protocol operations12
7.7.1 7.7.2	General 12 Request ID variation 12
7.7.2	Transport mappings 12
7.8.1	Port numbers 12
7.8.2	UDP over IPv4
7.8.3	UDP over IPv613
7.8.4	TCP over IPv4 13
7.8.5	TCP over IPv6
7.8.6	Secure transport 13
7.9	Management information base (MIB) 14
7.9.1	Agent MIBs
7.9.2	Notification originator MIBs
7.9.3	Proxy forwarder MIBs
7.9.4	
	

89-efef867e2d98/iso-prf-15784-2

<u>7.10</u>	Context engine ID discovery1	5
8	Performance1	5
8.1	<u>0verview</u> 1	
8.2	Default response time1	5
Anne	x A (informative) Primer for SNMP1	6
A.1	Overview1	
A.2	Object types	
A.3	SNMP objects	
A.4	SNMP messaging	7
<u>A.5</u>	Message contents1	8
<u>A.6</u>	_Communications layers1	8
Annex	x B (informative) Encoding examples1	9
B.1	Overview1	
B.2	GetRequest-PDU1	9
B.3	Response-PDU2	0
<u>B.4</u>	SNMPv3 SetRequest-PDU with authentication2	1
Biblio	graphy2	3
	vord	
0	Introduction	4
	Background	
0.2		
0.3	Document approach and layout	41.41 <i>)</i>
1	Scope	1
1	Normative references	W
2		2.
3	Terms and definitions	3
4	Symbols and abbreviated terms	4
1		
5	Conformance and Conventions	89-efef867e2d98/iso-prf-157
5.1	ASN.1)
5.2	SNMP Terminology	
5.3	Format	
5.4	Conformance	
6	Architecture	5
6.1	ITS services	5
6.2	Physical view	6
6.3	Communications view	6
7	Requirements	7
7.1	Overview	
7.2	Terminology and internal architecture	8
7.3	Message Processing and Dispatching	8
7.4	Applications	8
	Entity Type	
	Command Generator	8
7 4 2	Command Dogwooden	O Company

7.4.4	Notification Originator 8	
7.4.5	Notification Receiver9	
	Proxy Forwarder 9	
7.5	Security Models 9	
7.5.1	User-based Security Model 9	
7.5.2	Transport Security Model 10	
	View-based Access Control 10	
7.7	Protocol Operations 10	
7.7.1	General 10	
7.7.2	Request ID Variation 10	
7.8	Transport Mappings 10	
	Port numbers 10	
	UDP over IPv4 10	
	UDP over IPv6 10	
	TCP over IPv4	
	TCP over IPv6. 11	
	Secure Transport	
7.9	Management Information Base (MIB)	
	Agent MIBs 11	
	Notification Originator MIBs 12	
	Proxy Forwarder MIBs 12	
	Other supported data 12	
	Context Engine ID Discovery 12	
8	Performance 12	• \
8.1	Overview 12	1.211)
8.2	Default Response time	
Anne	A Primer for Protocol	
A.1	Overview 14	
<u>A.2</u>	Object Types14	
A.3	SNMP objects	
A.4	SNMP Messaging15	
A.5	Communications layers 150/PKF 15/04-2 16	
Annor	ottps://standards.iteh.ai/catalog/standards/iso/f8554c43-c751-4caa-b68 B Encoding Examples	9-efef867e2d98/iso-prf-15784-2
nime: B.1	Overview 17	*
в. 1 В.2	Get Request 17	
	Get Response 17	
	SNMPv3 Set Request with Authentication 18	
5.4	SNMFV3 Set Request With Authentication	
Riblio	graphy 20	

© ISO 2023 – 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.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.

This second edition cancels and replaces the first edition (ISO 15784-2:2015), which has been technically revised. It also incorporates the Amendment ISO 15784-2:2015/Amd-1:2020.

The main changes $\frac{improve\ security, are}{}$ as follows:

- support for Simple Network Management Protocol (SNMP) versions other than <u>SNMPv3SNMP version</u>
 3 have been removed;
- ——support for the Simple Transportation Management Protocol (STMP) has been removed;
- the security stack has been updated to support Transport Layer Security (TLS) version 1.3.

A list of all parts in the ISO 15784 series can be found on the ISO website.

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.

Field Code Changed

© ISO 2023 – All rights reserved

ISO/DISPRF 15784-2:2023(E2024(en)

Introduction

0.1 Background

The need for standardized communication with intelligent transport system (ITS) field devices is growing around the world. A number of countries base their field device communications on the Simple Network Management Protocol (SNMP).

There is a growing view and empirical evidence that standardizing this activity will result in improved ITS performance, reduced cost, reduced deployment time and improved maintainability. This document creates a standard for ITS field device communications based on several simple concepts:

- a) maximization of the use of the SNMP standards, which are widely used in the management of network devices:
- b) b) provision of a consistent definition of the transport and networking layers;
- c) c) promotion of the adoption of recommended security features; and
- d) d)—promotion of the use of interoperable data definitions for the management of field devices, such as those defined in the ISO 26048 series and regional standards while also supporting vendor and projectspecific data.

By using this approach, agencies can specify open procurement, and systems can be expanded geographically in an open and non-proprietary manner which reduces costs, accelerates deployment, and simplifies integration.

0.2 Overview

SNMP is a collection of planned and proven concepts and principles. SNMP employs the sound principles of abstraction and standardization. This has led to SNMP being widely adopted for communication between management systems and devices on the internet, and other communications networks.

This document requires the use of SNMP version 3 (SNMPv3), as defined by the Internet Engineering Task Force (IETF). SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure, previous versions of SNMP permit access control based on the unauthenticated contents of the SNMP message, rather than using the authenticated identity from the lower layers.

This document does not specify any requirements that contradict or cause non-conformance to the standards listed in the normative references section of this document.

The data to be exchanged by SNMP is defined in Management Information Bases (MIBs), which are defined separately in the firewall MIB, RFCs, the ISO 26048 series, regional standards, vendor specifications, and project specifications.

0.3 Document approach and layout

This document provides:

© ISO 2023 - All rights reserved

vii

- a) a)—an overview of itsthe content of SNMP, including conformance and conventions (Clause 5); (Clause 5):
- b) a description of the reference architecture for systems that implement this document (Clause 6); (Clause 6);
- c) e)—technical requirements for entities claiming conformance to this document (Clause 7); (Clause 7):
- d) d)-performance requirements for entities claiming conformance to this document (Clause 8); (Clause 8):
- e) e)—a primer for understanding the protocol defined in this document (see Annex A); Annex A):
- f) f)—example encodings of messages conforming to this document (see Annex B); Annex B):
- g) g)—an electronic profile requirements list for implementations to use (available at: https://standards.iso.org/iso/15784/-2/ed-2/en/); https://standards.iso.org/iso/15784/-2/ed-2/en/);
- h) an electronic management information base (MIB) that defines the firewall objects (available at: https://standards.iso.org/iso/15784/-2/ed-2/en/. https://standards.iso.org/iso/15784/-2/ed-2/en/).

iTeh Standards (https://standards.iteh.ai) Document Preview

ISO/PRF 15784-2

https://standards.iteh.ai/catalog/standards/iso/f8554c43-c751-4caa-b689-efef867e2d98/iso-prf-15784-2

© ISO 2023 – All rights reserved

∨iii

Intelligent transport systems	Data	exchange	involving	roadside
modules communication—_				

Part—

Centre to field device communications using Simple Network Management Protocol (SNMP)

1 Scope

This document specifies a mechanism for exchanging data and messages in the following cases:

- a) a)—exchange between a traffic management centre and ITS roadside equipment for traffic management;
- b) b) exchange between ITS roadside equipment used for traffic management.

This document is not applicable to:

- —communication between traffic management centres and in-vehicle units;
- —communication between ITS roadside equipment and in-vehicle units;
- —in-vehicle communication;
- —in-cabinet communication;
- motion video transmission from a camera or recorded media.

This document is suitable for use when both of the following conditions apply:

- 1) The data to be exchanged can be defined as one or more elements that can be retrieved or stored SNMP can support a wide variety of devices and has adopted the concept of a management information base (MIB), which identifies the configuration, control and monitoring parameters for ITS roadside equipment. This standardized approach is commonly used for network management applications for devices such as routers, switches, bridges and firewalls. It is also used in many regions to control devices such as dynamic message signs.
- 2) —Guaranteed, deterministic, real-time exchange of data is not critical SNMP operations typically require less than 100ms 100 ms, but the underlying network can cause multi-second delays in delivering messages or even lost messages; thus, SNMP is not intended for applications that require reliable subsecond communications.

This document can be used for:

- —intermittent exchange of any defined data (normal SNMP operations allow messages to be structured by combining any group of elements into a retrieval or storage request);
- repeated, frequent exchanges of the same message structure (with potentially different values), even on relatively low-bandwidth links;

NOTE_1 The dynamic object feature, defined in ISO<u>/TS</u> 26048-1, can be used to eliminate a considerable amount of overhead that is normally associated with SNMP communications to make it more suitable for low-bandwidth links.

— allowing ITS roadside equipment to issue exception reports when special conditions arise.

NOTE_2- Exception reporting uses SNMP notifications in combination with the notification management features defined in ISO $\underline{\text{TS}}$ 26048-1.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO<u>/TS</u> 14812, Intelligent transport systems — Vocabulary

ISO/TS 26048-1, Intelligent transport systems —_Field device SNMP data interface —Part 1: Global objects

RFC 2578, Structure of Management Information Version 2 (SMIv2), April 1999-

RFC 2579, Textual Conventions for SMIv2, April 1999-

RFC 2580, Conformance Statements for SMIv2, April 1999. 16h Standards

RFC 3411, An Architecture for Describing SNMP Management Frameworks, December 2002-

RFC 3412, Message Processing and Dispatching, December 2002-

RFC 3413, SNMP Applications, December 2002.

RFC 3414, User-based Security Model, December 2002-

RFC 3415, View-based Access Control Model, December 2002-

RFC 3416, Version 3416Version 2. of SNMP Protocol Operations, December 2002-

RFC 3417, Transport Mappings, December 2002-

2

RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002_7

RFC 3430, Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping, December 2002-

RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model, June 2004:

RFC 4001, Textual Conventions for Internet Network Addresses, February 2005

RFC 5590, Transport Subsystem for the Simple Network Management Protocol (SNMP), June 2009-

RFC 5591, Transport Security Model for the Simple Network Management Protocol (SNMP), June 2009-

© ISO 2023 All rights reserved

© ISO 2024 - All rights reserved

RFC 6353, Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), July 2011-

RFC 7860, HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3, April 2016

RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018

RFC 9147, The Datagram Transport Layer Security (DTLS) Protocol Version 1.3, April 2022

RFC 9456, Updates to the TLS Transport Model for SNMP, November 2023-

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 14812 and the following 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

agent

Simple Network Management Protocol (SNMP) entity that can respond to SNMP get and set requests

Note_1_to_entry:_An agent may also issue report, trap and/or inform messages.

3.2

datagram

self-contained unit of data transmitted independently of other units of data

3.3

deprecated

still valid, but not to be used for new designs

Note-1-to-entry:-This is a term that is used in the STATUS field of management information bases (MIBs) to indicate that the associated object type no longer represents the preferred design, but the object type can still be useful for backwards compatibility with legacy implementations. A deprecated object type can be made obsolete with the next, or subsequent, release of the standard.

3.4

encoding

complete sequence of octets used to represent a data value

3.5

field device

infrastructure-based ITS component located outside of a data centre that is designed to provide local processing or routing services while stationary

Note_1-to_entry:-This concept is described in ISO<u>/TS</u> 14812 using the term "field system". However, this document uses the term "field device" due to the use of the latter term in management information base (MIB) modules that pre-date the ISO<u>/TS</u> 14812 definition.

© ISO 2023 All rights reserved

3