



BSI Standards Publication

Intelligent transport systems — Criteria for privacy and integrity protection in probe vehicle information systems

National foreword

This British Standard is the UK implementation of ISO 16461:2018.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 88586 0

ICS 03.220.01; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

ISO
16461

First edition
2018-08-01

Intelligent transport systems — Criteria for privacy and integrity protection in probe vehicle information systems

*Systèmes intelligents de transport — Critères de confidentialité et de
protection d'intégrité*



Reference number
ISO 16461:2018(E)
Documents
Document Sharing Hub
© ISO 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	4
5 Reference architecture	5
5.1 Reference architecture for probe vehicle systems	5
5.2 Context model for privacy and data integrity protection	5
6 Basic framework	5
6.1 Overview	5
6.2 Structure of framework	5
6.3 Index framework	6
6.4 Category framework	6
6.5 Application of evaluation framework on probe vehicle systems	7
6.5.1 Anonymity (FPR_ANO)	7
6.5.2 Pseudonymity (FPR_PSE)	8
6.5.3 Unlinkability (FPR_UNL)	9
6.5.4 Unobservability (FPR_UNO)	10
6.5.5 Integrity of exported TSF data (FPT_ITI)	10
7 Criteria for privacy protection	10
7.1 Overview	10
7.2 Raw sensor data processing	10
7.3 Probe data retention	11
7.4 Probe message creation	11
7.5 Probe package creation	12
7.6 Probe package reception	13
7.7 Probe package processing	13
7.8 Processed probe data retention	14
7.9 Probe information creation	15
Bibliography	16

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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

More and more attention has been paid to safety, comfort, mitigation of impact on the environment, and energy efficiency in transport systems. The use of probe data specified in [ISO 22837:2009](#) is considered to be a key factor of a solution for the above issues. Usage of probe data in probe vehicle systems (PVS), defined in [ISO 22837:2009](#), may be subject to privacy regulations. Consequently, there is a need for protective measures and policies in PVS.

It is necessary to develop a basic concept for protecting privacy and integrity being gathered in the PVS so that transmission of probe data can be done without violating the privacy regulations. This document defines criteria for protection of the anonymity and integrity of probe data.

The following topics are addressed in this document:

- definition of security and privacy requirements for probe vehicle systems;
- specification of a common interface ensuring privacy and integrity in probe vehicle information acquisition;
- definition of a scheme for protecting probe vehicle systems in terms of integrity and privacy.

This page deliberately left blank