PD ISO/TR 17427-7:2015

BSI Standards Publication

Intelligent transport systems — Cooperative ITS

Part 7: Privacy aspects

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of ISO/TR 17427-7:2015.

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 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 87424 6
ICS 03.220.01; 35.240.60

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/TR 17427-7:2015

TECHNICAL REPORT

ISO/TR 17427-7

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 7: Privacy aspects

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 7: Aspects relatifs à la vie privée

Reference number
ISO/TR 17427-7:2015(E)

Documents
Document Sharing Hub
© ISO 2015

Full document details: PD ISO/TR 17427-7:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, 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

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 17427-7:2015

Contents

Page

Foreword ... **iv**
Introduction ... **vi**
1 Scope ... **1**
2 Terms and definitions ... **1**
3 Abbreviations and acronyms ... **2**
4 How to use this Technical Report ... **2**
4.1 Acknowledgements ... 2
4.2 Guidance ... 3
4.3 ITS and 'Privacy' ... 3
4.4 C-ITS 'Privacy' issues ... 4
4.4.1 General C-ITS 'Privacy' issues ... 4
4.4.2 Examples of vehicle tracking ... 6
4.4.3 Anonymity ... 6
4.4.4 Deployment models ... 8
5 C-ITS Actors and Privacy ... **9**
5.1 C-ITS and jurisdictions ... 9
5.1.1 United States ... 9
5.1.2 Europe ... 10
5.1.3 Australia ... 12
5.1.4 Other countries ... 14
5.1.5 International Standards ... 14
5.1.6 Privacy and governments ... 14
5.2 C-ITS and road operators/managers ... 15
5.2.1 Jurisdictions ... 15
5.2.2 'Core' systems ... 16
5.3 C-ITS and manufacturers ... 16
5.4 C-ITS information/application service providers ... 16
5.5 C-ITS, drivers and vehicle owners ... 17
5.6 Further reading ... 17
5.7 Aspects relating to probe vehicle information services ... 17
6 Policy questions and approaches ... **17**
6.1 Is specific regulation required for C-ITS? ... 17
6.1.1 Option 1: Continue current approach ... 17
6.1.2 Option 2: Privacy code ... 18
6.1.3 Option 3: Provide guidance on best practice ... 18
6.1.4 Option 4: Legislate C-ITS governance arrangements and use of information ... 18
6.1.5 Option 5: Legislate technical standards to protect privacy ... 18
6.1.6 Option 6: Match and copy mobile phone privacy measures ... 18
7 Summary of findings ... **19**
7.1 General ... 19
7.2 Principal opinions ... 20
7.3 Privacy — Private Sector ... 22
7.4 Privacy — Public Sector ... 22
Bibliography ... **23**

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

ISO 17427 consists of the following parts, under the general title *Intelligent transport systems — Cooperative ITS*:

— *Part 2: Framework Overview* [Technical Report]

— *Part 3: Concept of operations (ConOps) for 'core' systems* [Technical Report]

— *Part 4: Minimum system requirements and behaviour for core systems* [Technical Report]

— *Part 6: 'Core system' risk assessment methodology* [Technical Report]

— *Part 7: Privacy aspects* [Technical Report]

— *Part 8: Liability aspects* [Technical Report]

— *Part 9: Compliance and enforcement aspects* [Technical Report]

— *Part 10: Driver distraction and information display* [Technical Report]

The following parts are under preparation:

— *Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)*

— *Part 5: Common approaches to security* [Technical Report]

— *Part 11: Compliance and enforcement aspects* [Technical Report]

— *Part 12: Release processes* [Technical Report]

— *Part 13: Use case test cases* [Technical Report]

— *Part 14: Maintenance requirements and processes* [Technical Report]

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015

Further technical reports in this series are expected to follow. Please also note that these TRs are expected to be updated from time to time as the C-ITS evolves.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015

Introduction

Intelligent transport systems (*ITS*) are transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort.

A distinguishing feature of '*ITS*' are its communication with outside entities.

Some *ITS* systems operate autonomously, for example 'adaptive cruise control' uses radar/lidar/and/or video to characterize the behaviour of the vehicle in front and adjust its vehicle speed accordingly. Some *ITS* systems are informative, for example 'Variable Message Signs' at the roadside, or transmitted into the vehicle, provide information and advice to the driver. Some *ITS* systems are semi-autonomous, in that they are largely autonomous, but rely on 'static' or 'broadcast' data, for example, *GNSS* based 'SatNav' systems operate autonomously within a vehicle but are dependent on receiving data broadcast from satellites in order to calculate the location of the vehicle.

Cooperative Intelligent Transport Systems (*C-ITS*) are a group of *ITS* technologies where service provision is enabled by, or enhanced by, the use of 'live', present situation related, dynamic data/information from other entities of similar functionality (for example from one vehicle to other vehicle(s)), and/or between different elements of the transport network, including vehicles and infrastructure (for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)). Effectively, these systems allow vehicles to 'talk' to each other and to the infrastructure. These systems have significant potential to improve the transport network.

A distinguishing feature of '*C-ITS*' is that data are used across *application*/service boundaries.

It will be immediately clear to the reader that such systems present the possibility to seriously compromise privacy, and must, and will, be strictly controlled by regulation and managed to prevent abuse of privacy by any party. The purpose of this Technical Report is to identify potential critical privacy issues that *C-ITS* service provision may introduce, to consider how to control, limit or mitigate such privacy issues, and to limit the risk of exposure to the financial consequences of privacy issues.

This Technical Report is a 'living document' and as our experience with *C-ITS* develops, it is intended that it will be updated from time to time, as and when we see opportunities to improve this Technical Report.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015

Intelligent transport systems — Cooperative ITS —

Part 7:
Privacy aspects

1 Scope

The scope of this Technical Report is as an informative document to identify potential critical privacy issues that *C-ITS* service provision may introduce; to consider strategies for how to control, limit or mitigate such privacy issues; and to give pointers, where appropriate, to standards deliverables existing that provide specifications for all or some of these aspect and to limit the risk of exposure to the financial consequences of privacy issues.

The objective of this Technical Report is to raise awareness of and consideration of such issues. This Technical Report does not provide specifications for solutions of these issues.

2 Terms and definitions

2.1
application
app
software application

2.2
application service
service provided by a service provider accessing data from the *IVS* (2.6) within the vehicle in the case of *C-ITS*, via a wireless communications network, or provided on-board the vehicle as the result of software (and potentially also hardware and firmware) installed by a service provider or to a service providers instruction

2.3
cooperative ITS
C-ITS
group of *ITS* technologies where service provision is enabled, or enhanced by, the use of 'live', present situation related, data/information from other entities of similar functionality [for example, from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure

[SOURCE: for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)]

2.4
core system
combination of enabling technologies and services that will provide the foundation for the support of a distributed, diverse set of *applications* (2.1), and *application* transactions which work in conjunction with 'External Support Systems' such as 'Certificate Authorities'

Note 1 to entry: the system boundary for the core system is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behaviour of all interactions between core system users

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 17427-7:2015

2.5
global navigation satellite system
GNSS
comprises several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe

2.6
intelligent transport systems
IVS
hardware, firmware and software on board a vehicle that provides a platform to support *C-ITS* service provision, including that of the *ITS-station* (2.8) (ISO 21217), the facilities layer, data pantry and on-board 'apps'

2.7
in-vehicle system
ITS
transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort

2.8
ITS-station
entity in a communication network [comprised of *application* (2.1), facilities, networking and access layer components] that is capable of executing *ITS-S application* processes, comprised of an *ITS-S* facilities layer, *ITS-S* networking & transport layer, *ITS-S* access layer, *ITS-S* management entity and *ITS-S* security entity, which adheres to a minimum set of security principles and procedures so as to establish a level of trust between itself and other similar *ITS-station*s with which it communicates

3 Abbreviations and acronyms

ANPR	automatic number plate recognition
EDR	electronic data recorder
C-ITS	cooperative intelligent transport systems, cooperative ITS
IPP	information privacy principle
ITS	intelligent transport systems (2.6)
IVS	*in-vehicle system* (2.7)
NPP	National privacy principle
TR	technical report
V2V	vehicle to vehicle

4 How to use this Technical Report

4.1 Acknowledgements

Much of the inspiration for this Technical Report and its considerations and content originate from the reports "*Cooperative ITS Regulatory Policy Issues*" and "*Cooperative Intelligent Transport Systems Policy Paper*" National Transport Commission, Australia. And this source is acknowledged and thanked.[1][17]

Contribution from various TCA (Transport Certification Australia) documents are acknowledged.

Contribution from the report of EC Project PRECIOSA is acknowledged.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015

Contribution from the US DoT document "CoreSystem_SE_SyRS_RevF" is acknowledged.

The review by the office of the European Data Protection Supervisor is acknowledged and thanked

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning privacy associated with the deployment of *C-ITS* service provision. It does not purport to be a list of all potential privacy factors – which will vary according to the regime of the jurisdiction, the location of the instantiation, and to the form of the instantiation, nor does it provide definitive specification. Rather this TR discusses and raises awareness of the major issues to be considered, and provides guidance and direction for considering and managing privacy in the context of future and instantiation specific deployment of *C-ITS*.

4.3 ITS and 'Privacy'

Privacy is the subject of National Regulation, but most countries have signed up to one or more of OECD, APEC and/or European Union principles for personal privacy.

The subject of how 'privacy' regulations affect *ITS*, the variations of 'privacy' regulations around the world, and general measures that *ITS* should adopt in respect of 'privacy' and *ITS* are dealt with in ISO/TR 12859.

Suffice to say, in summary that ISO/TR 12859 recommends that the conditions under which data shall be collected and held in support or provision of *ITS* services shall uphold all of the following principles:

a) Avoidance of harm	Recognize the interests of the individual to legitimate expectations of privacy, personal information protection; prevent the misuse of such information. Further, acknowledging the risk that harm may result; take account of such risk, and remedial measures should be proportionate.
b) Fairly and lawfully	Personal data obtained and processed fairly and lawfully.
c) Specified, explicit and legitimate purposes	Personal data collected for specified, explicit and legitimate purposes.
d) Explicit and legitimate and must be determined at the time of collection of the data	Purposes for which personal data are collected shall be determined at the time of the collection of the data and shall be explicit and legitimate at the time of collection of the data and use and subsequent of the data limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes specified); All personal data collected shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.
e) Not further processed in a way incompatible with the purposes for which it was originally collected	Personal data shall not be further processed or used in a way incompatible with the purposes for which it was originally collected.
f) Not be disclosed without the consent of the data subject	Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified.
g) Adequate, relevant and not excessive in relation to the purposes for which they are collected	Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
h) Accurate and, where necessary, kept up to date	Personal data shall be accurate and kept up to date; every reasonable step must be taken to erase or rectify inaccurate or incomplete data, having regard to the purposes for which they were collected.
i) Identification of data subjects for no longer than is necessary for the purposes for which the data were collected	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
j) Restricted to those who have a demonstrable 'need to know'	The use of personal data to be restricted to those who have a genuine need to know.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 17427-7:2015