ETSI TR 187 020 V1.1.1 (2011-05)

Technical Report

Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436

Reference
DTR/TISPAN-07044

Keywords
privacy, RFID, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

CEN and CENELEC have based their IPR policy on that of ISO, IEC and ITU-T. Patents or pending patent applications relating to a CEN or CENELEC publication may have been declared on this basis to CEN or CENELEC. Information on these declared patents or pending patent applications is made available by CEN and CENELEC via an on-line list of declarations (ftp://ftp.cen.eu/CEN/WorkArea/IPR/Patents.pdf).

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). The present document has been prepared under the coordination of a technical experts group composed of representatives of each of ETSI, CEN and CENELEC and represents the agreed response of the European Standards Organizations (ESOs) to Mandate M/436 on the subject of Radio Frequency Identification Devices (RFID) in relation to data protection, information security and privacy.

NOTE: This work was funded under EC/EFTA Contract reference SA/ETSI/ENTR/436/2009-02.

1 Scope

The present document provides the results of the coordinated response of the European Standards Organizations (ESOs) to Phase 1 of EC mandate M436 on the subject of Radio Frequency Identification Devices (RFID) in relation to privacy, data protection and information security.

The present document outlines a standardization roadmap for privacy and security of RFID. The development of the roadmap involved analyses of RFID from a number of perspectives:

- analysis of OECD guidelines [i.17] and relevant data protection;
- analysis of privacy and its link to behaviour;
- analysis of EU directives on data protection and privacy and their implications on RFID;
- review of the role of PETs for RFID (see clause 7); and
- analysis of security threats to RFID and their implications (see Annex C).

The resulting requirements set defines the data protection, privacy and security needs of RFID and was used as input to the standards gaps analysis and the development of requirements to PIA for RFID and RFID PEN testing frameworks. An outline of the PIA framework requirements is given in clause 9.

Overview of the standardization gaps and requirements for RFID PEN testing is given in clause 10. The standardisation gaps analysis and resulting overall RFID standardisation roadmap is given in clause 4.

The present document recommends a plan of activities for Phase 2 of EC Mandate M436 as follows:

- identifies the use of existing technical measures described by standardisation in order to promote confidence and trust (by end users organizations and the general public) in RFID technology and its applications;
- identifies where new technical measures described by standardisation are required in order to promote confidence and trust (by end users organizations and the general public) in RFID technology and its applications. These measures will be developed in the course of phase 2 of the mandate.

In addition the present document describes the results of modelling the role of RFID in privacy and personal data as defined by European Directives alongside a Threat Vulnerability and Risk Analysis (TVRA) of the use of RFID technology and its applications, including the results of a generic and an industry specific Privacy Impact Assessment (a guide to PIA is given in Annex A).

NOTE: Many of the risks identified as part of the present document are equally applicable in other tracking scenarios (e.g. CCTV, car number/licence plate recognition, face recognition, mobile phone cell tracking). Under the terms of the Mandate, the present document covers only those areas in the data acquisition part that are specific to RFID. The other tracking scenarios are included in the work of the Article 29 Data Protection Working Party.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.