SIST

SLOVENSKI STANDARD
SIST-TP CEN/TR 16671:2014

01-september-2014

Informacijska tehnologija - Dovoljenje za uporabo mobilnih telefonov kot RFID-bralnikov

Information technology - Authorisation of mobile phones when used as RFID interrogators

Informationstechnik - Autorisierung von Mobilfunkgeräten als RFID-Lesegeräte

Technologie de l'information - Autorisation des téléphones mobiles utilisés comme interrogateurs RFID

Ta slovenski standard je istoveten z: CEN/TR 16671:2014

ICS:

33.070.01	Mobilni servisi na splošno	Mobile services in general
35.020	Informacijska tehnika in tehnologija na splošno	Information technology (IT) in general

SIST-TP CEN/TR 16671:2014 **en,fr,de**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1de2a-a344-488e-b6bd-614a7329e9e/sist-tp-cen-tr-16671-2014

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1dbe2a-a344-488e-b6bd-614a732dfa9e/sist-tp-cen-tr-16671-2014

SIST-TP CEN/TR 16671:2014

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16671

June 2014

ICS 35.240.60; 33.070.01

English Version

Information technology - Authorization of mobile phones when used as RFID interrogators

Technologies de l'information - Autorisation des téléphones mobiles utilisés comme lecteurs RFID

Informationstechnik - Autorisierung von Mobilfunkgeräten als RFID-Lesegeräte

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1dbe2a-a34-488e-b6bd-614a732dfa9e/sist-tp-cen-tr-16671-2014

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TR 16671:2014 E

SIST-TP CEN/TR 16671:2014

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5f1ebe2a-a144-488e-b9d-014a732afa9e/sist-tp-cen-tr-16671-2014

SIST-TP CEN/TR 16671:2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1dbe2a-a344-488e-b6bd-614a732dfa9e/sist-tp-cen-tr-16671-2014

SIST-TP CEN/TR 16671:2014

Foreword

This document (CEN/TR 16671:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC technologies”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This Technical Report is one of a series of related deliverables, which comprise mandate 436 Phase 2. The other deliverables are:

— EN 16570, *Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application systems*

— EN 16571, *Information technology — RFID privacy impact assessment process*

— EN 16656, *Information technology - Radio frequency identification for item management - RFID Emblem (ISO/IEC 29160:2012, modified)*

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

— CEN/TS 16685, *Information technology — Notification of RFID — The information sign to be displayed in areas where RFID interrogators are deployed*

— CEN/TR 16669, *Information technology — Device interface to support ISO/IEC 18000-3 Mode 1*

— CEN/TR 16670, *Information technology — RFID threat and vulnerability analysis*

— CEN/TR 16672, *Information technology — Privacy capability features of current RFID technologies*

— CEN/TR 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

— CEN/TR 16674, *Information technology — Analysis of privacy impact assessment methodologies relevant to RFID*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/61dbe2a-a3d-48e-b6b2-6144a92dfa9e/sist-tp-cen-tr-16671-2014

SIST-TP CEN/TR 16671:2014

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96 'RFID in Europe: steps towards a policy framework'. This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardisation work programme identified in the first phase.

This Technical Report explores developments in the use of mobile phones as RFID interrogators. The integration of Near Field Communication (NFC) in mobile phones, many years ago, has enabled mobile phones for use as RFID interrogators. NFC is generally considered to be a close-coupled mechanism with a defined operating distance of maximum 10 cm. Recently the NFC Forum, amongst other things formed to advance the use of NFC technology by developing specifications, has started developments to extend the support for NFC tag types in the phones to also support tags that are compliant to ISO/IEC 15693 and ISO/IEC 18000-3 Mode 1.

Another recent development is the integration of Ultra High Frequency (UHF) reader chips into mobile phones. That allows using mobile phones as interrogators to read UHF tags, for example UHF tags that are compliant with ISO/IEC 18000-63 or the equivalent GS1 UHF EPC Gen2 standard. It is also realistic to expect that in the future mobile phones might appear that have combined support for both NFC and UHF technology.

These new additions have the potential to increase the read range and might enable NFC and UHF mobile phones to capture data without consent from RFID tags and ID badges compliant with these well-established standards.

By nature mobile phones are connected to the GSM network that provides an access portal to the Internet of Things (IoT). In addition modern mobile phones become equipped with strong processors that have the potential to manipulate data. The ability to use the mobile phone as RFID Interrogators to surreptitiously read data, the increased computing power and the access portal to the IoT can potentially ruin the efficacy of an RFID application.

This Technical Report describes emerging developments in the functionality of mobile phones and analyses the risks that these developments could have on the privacy and security aspects.

SIST-TP CEN/TR 16671:2014

1 Scope

The scope of this Technical Report is to explore developments in the use of mobile phones as RFID interrogators. It uses as a datum the communication protocols developed for near field communication, which have a defined level of security. This Technical Report will explore known developments in the use of mobile phones as RFID interrogators including (but not limited to):

— extending NFC phone capabilities to read RFID tags compliant with ISO/IEC 15693 and ISO/IEC 18000-3 Mode 1;

— using mobile phones as interrogators for UHF tags based on ISO/IEC 18000-6 Type C;

— the development of multi-protocol readers capable of switching between high frequency and UHF.

The objective of the Technical Report is to identify specific characteristics associated with mobile phones being used as interrogators with tags that are primarily intended for other purposes. It will identify some potential threats associated with the technology. It will also identify gaps in the standardization process that might need to be addressed to mitigate against such threats.

To counterbalance any negative implications, the Technical Report also identifies real and potential applications that could lead to an accelerated take-up of RFID and the Internet of Things through mobile phones being used as RFID interrogators by individual citizens and organizations.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1dbe2a-a444-488e-b6b6-614a732dfa9e/sist-tp-cen-tr-16671-2014

2 Normative references

Not applicable

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
anti-collision loop
algorithm used to prepare for dialogue between PCD and one or more PICCs out of the total number of PICCs responding to a request command

3.2
contactless
pertaining to the achievement of signal exchange with and supplying power to the card without the use of galvanic elements

EXAMPLE The absence of an ohmic path from the external interfacing equipment to the integrated circuit(s) contained within the card.

3.3
contactless integrated circuit(s) card
card of the card type ID-1 into which integrated circuit(s) have been placed and in which communication to such integrated circuit(s) is done in a contactless manner

[SOURCE: ISO/IEC 7810]

SIST-TP CEN/TR 16671:2014

3.4
integrated circuit
IC
electronic component designed to perform processing and/or memory functions

3.5
NFC forum
near Field Communication Forum that was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology

3.6
PCD
proximity coupling device
a reader/writer device that uses inductive coupling to provide power to the PICC and also to control the data exchange with the PICC

3.7
PICC
proximity integrated circuit card
a card type ID-1 into which integrated circuit(s) and coupling means have been placed and in which communication to such integrated circuit(s) is done by inductive coupling in proximity of a coupling device

3.8
PICC mode
mode in which NFCIP-2 device operates as Type A or Type B Proximity Integrated Circuit Card or Object as specified in ISO/IEC 14443

3.9
PCD mode
mode in which NFCIP-2 device operates as Proximity Coupling Device as specified in ISO/IEC 14443

3.10
VCD mode
mode in which NFCIP-2 device operates as Vicinity Coupling Device as specified in ISO/IEC 15693

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f1dbe2a-a34e-488e-b6bd-614a732d1a0a/sist-tp-cen-tr-16671-2014

4 Symbols and abbreviations

CMOS Complementary Metal Oxide Semiconductor

HF High Frequency

IoT Internet of Things

kbit/s kbit per second

NOTE data rate unit

NFC Near Field Communication

OOK On Off keying

PCD Proximity Coupling Device

PICC Proximity Integrated Circuit Card

RFID Radio Frequency IDentification

UHF Ultra High Frequency

SIST-TP CEN/TR 16671:2014

5 Executive summary and conclusions

This document reports the potential impact that mobile phones can have when they are used as interrogators to read tags that are primarily intended for other purposes.

The NFC Forum has started a new work item planning to add ISO/IEC 15693 into their specification, including a new Type Tag Platform. Therefore in the future NFC phones might get capabilities to read and write ISO/IEC 15693 compliant RFID tags. The analysis in this report leads to the conclusion that the introduction of the new capability will increase the number of tags that an NFC phone can read. However, it will not have an impact on the read range of the existing ISO/IEC 14443 based tags and therefore it will not increase the capabilities of NFC mobile phones to capture data without consent from RFID tags and ID badges that are currently in the field.

The capability to read and write to ISO/IEC 15693 compliant tags might cause a threat for applications that currently use such tags. This point requires special attention for the privacy impact assessment of a new RFID application where these tags will be applied.

The report also analysed potential capabilities to extend the read range for current NFC tags. The theoretical analysis showed that it is practically impossible to extend the range of an existing NFC phone. That conclusion is confirmed by attempts to extend the read range by changing the environment of applying specific hardware like a special booster.

Extending the phones with UHF capabilities can potentially be a threat for the consumer's privacy. The evaluation of such phones shows that the availability is currently only for industrial use. There are a few phones that support the UHF RFID protocols EPCglobal UHF C1G2, ISO/IEC 18000 Type B, ISO/IEC 18000-6 Type C and the HF protocol ISO/IEC 14443 Type A, but the threat for the consumer privacy appears to be less than the threat caused by the availability of dedicated UHF handheld readers.

The impact of the development of multi-protocol readers that are capable of switching between HF and UHF will be similar to the impact of the individual HF or UHF technology. A combination of both technologies will not add more threats for the consumers' privacy.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0fbe2ea-a344-488e-b0dd-614a732dfa98/sist-tp-cen-tr-16671-2014

6 Extending NFC phones capabilities to read RFID tags

NOTE This clause summarizes the evaluation of developments in using mobile phones as RFID interrogators.

6.1 Read range impacts due to inclusion of ISO/IEC 15693

6.1.1 Short introduction to NFC

NFC is a short-range, wireless connectivity technology that allows consumers to perform safe, contactless transactions, access digital content, and connect electronic devices with the simplicity of a touch. Consumers with NFC-enabled mobile phones may, for example, leave their wallets at home and use their phones to conduct contactless financial transactions, or to gain electronic access to public transportation.

Tags are cards or labels with integrated circuits that store data that can be read by NFC-enabled devices to support these applications. For example, a cinema goer with an NFC-enabled mobile phone may touch a movie poster containing an embedded NFC tag to view a preview of the movie on the phone or to purchase a ticket for watching the movie in a cinema.

NFC signal interfaces and protocols are specified in standards. The fundamentals of NFC are specified in ISO/IEC 18092 containing a protocol to exchange data between two devices. The communication link is based on ISO/IEC 14443 Type A and Japanese Industrial Standard (JIS) X 6319-4 (also known as Sony's FeliCa). The interoperability extensions of NFC are specified in ISO/IEC 21481 and include full ISO/IEC 14443

SIST-TP CEN/TR 16671:2014

card (PICC) and Reader/Writer (PCD) support, as well as JIS X 6319-4 card and Reader/Writer support as well as ISO/IEC 15693 reader support.

Although ISO/IEC 18092, ISO/IEC 14443 and ISO/IEC 15693 all specify 13,56 MHz as their working frequency, they specify distinct physical layer and distinct communication protocols.

ISO/IEC 21481 also specifies the mechanism to detect and select the communication mode based on the features of the devices involved in the communication.

Additionally the standards do include a collision avoidance to avoid potential disturbance of any ongoing communication for devices that are compliant with ISO/IEC 18092, ISO/IEC 14443 or ISO/IEC 15693.

6.1.2 NFC Forum and NFC Forum tag types

The NFC Forum was formed to advance the use of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. The members of the NFC Forum all work together to promote the use of NFC technology in consumer electronics, mobile devices, and PCs.

NFC Forum is promoting interoperability of NFC-enabled devices by setting interoperability standards including the features to be supported as well as test methods combined in a compliance program allowing manufactures to certify devices. One part of those efforts focuses on accessing data and information stored on passive tags. To accomplish that the NFC Forum has standardized so called operation specifications describing how an NFC Forum Device can read and write relevant data for four globally relevant Type Tag Platforms. The signal interfaces and protocols used by the four platforms are compliant with ISO/IEC 21481. The mandate to support access to all four Type Tag Platforms by NFC Forum Devices is the backbone of interoperability between NFC tag providers and NFC Forum Device manufacturers. It ensures a uniform user experience. The coding of the information to be stored and the actual data format being used on such Type Tag Platforms is standardized by the NFC Forum as well. This is specified in the NFC Data Exchange Format (NDEF) specification and four Record Type Description (RTD) specifications. They are available for download at www.nfc-forum.org/specs/.

The operation specifications for the NFC Forum tag types, numbered 1-4, provide the technical information required to implement the reader/writer and associated control functionality of an NFC Forum Device, enabling interaction with the tags. The four specifications are:

— Type 1 tag is based on ISO/IEC 14443 Type A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability on actual products is typically 96 bytes; communication speed is 106 kbit/s.

— Type 2 tag is based on ISO/IEC 14443 Type A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability on actual products is in the range from 48 bytes to 2 KByte; communication speed is 106 kbit/s.

— Type 3 tag is based on JIS X 6319-4. Tags are pre-configured at manufacture to be either read and re-writable, or read-only. Memory availability on actual products is variable, typical ranges are a few hundred bytes up to a few KBytes; communication speed is 212 kbit/s or 424 kbit/s.

— Type 4 tag is based on ISO/IEC 14443 (Type A and Type B). Tags are pre-configured at manufacture to be either read and re-writable, or read-only. Memory availability on actual products is variable, up to 32 KBytes per service; communication speed is up to 424 kbit/s.

6.1.3 Inclusion of support for ISO/IEC 15693

Recently the NFC Forum has started a new work item planning to add ISO/IEC 15693 into their specification including a new Type Tag Platform based on this same technology.

SIST-TP CEN/TR 16671:2014

6.1.4 NFC Forum directive on ISO/IEC 15693 capability extension

NFC technology is generally considered to be a close-coupled mechanism with a typical operating volume of a few centimeters. The maximum operating volume known from ISO/IEC 14443 based systems is up to 10 cm. As the NFC Forum is now extending the functionality with ISO/IEC 15693 is raises the concern that the read capability could potentially grow with the support of ISO/IEC 15693 that in typical use provides a longer read range.

The NFC Forum Board of Directors has issued the following directive on this issue:

— the Board confirms that the ISO 15693 VCD Mode (as proposed in a New Work Item according to their processes) is within the scope of the NFC Forum;

— the Technical Committee (the organisational part that manages the technical specifications) shall take into consideration for this and all future activities that a key feature of NFC technology is a “touch based” user experience, characterised by a limited working distance (usually around 4cm to 10cm), which needs to be reflected in any specifications where applicable.

6.1.5 Analysis of ISO/IEC 15693 tag type extension

The inclusion of ISO/IEC 15693 and a related new Type Tag Platform will not have an influence on the performance of the mobile phone to read existing tags. In fact the majority of the modern NFC enabled phone already use NFC reader ICs that are compliant with ISO/IEC 21481 (NFCIP-2) and for those phones there will be no difference (in read range) at all.

Some of the NFC enabled phones that are compliant with ISO/IEC 21481 (NFCIP-2) can already read and write ISO/IEC 15693 tags. Adding support for the new 15693 NFC Forum tag type will increase the interoperability with NFC Forum devices, but will not have a consequence for the read range for reading existing tags.

NFC phones can read ISO/IEC 14443 (proximity) tags and ISO/IEC 15693 (vicinity) tags. Loosely speaking an ISO/IEC 15693 tag is designed to offer larger reading distances and as a consequence in general has less functionality than an ISO/IEC 14443 tag. The architecture of the ISO/IEC 15693 tags is less complex and therefore the tag needs less power to operate. The minimum operating field strength of ISO/IEC 15693 is 150 mA/m and the minimum operating field of ISO/IEC 14443 is 1500 mA/m. So the ISO/IEC 15693 tags need ten times less power than the ISO/IEC 14443 tag and for that reason the ISO/IEC 15693 tags can be read at a larger distance.

EXAMPLE A test with a Google Nexus S NFC phone shows that an ISO/IEC 14443 card can be read at: 2,5 cm. The same phone can read an ISO/IEC 15693 card under the same circumstances at 7 cm.

This analysis leads to the conclusion that the introduction of a new ISO/IEC 15693 NFC forum tag type will increase the number of tags that an NFC phone can read. It will not have an impact on the read range of the existing ISO/IEC 14443 based tags and therefore it will not increase the capabilities of NFC mobile phones to capture data without consent from RFID tags and ID badges that are currently in the field.

NOTE The fact that many modern NFC phones can read and write ISO/IEC 15693 tags forms a potential threat for the privacy and security of existing systems that use ISO/IEC 15693 tags.

The inherent larger reading distance of ISO/IEC 15693 tags should get special attention in a privacy impact assessment for an RFID system where these tags will be applied.

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/6f1dbe73-a444-4886-b0b1-d44a32a8a9e/sist-tp-cen-tr-16671-2014