Standardization Trends in Proximity Contactless Communication Technology

Hideaki Yamamoto, Kimihiro Yamakoshi, and Tetsushi Morita

Abstract

Services using proximity contactless communication such as NFC-enabled smartphones and contactless IC cards have been widely used in recent years (NFC: near field communication, IC: integrated circuit). We introduce the trends in proximity contactless communication technology from the viewpoint of international standardization.

1. Introduction

1.1 Short-range communication

Proximity contactless communication is defined as interactive communication technology in which the maximum communication distance is approximately 10 cm when using a magnetic field of 13.56 MHz. This technology has become prevalent in systems used for such services as access control, railway ticketing, and electronic payment.

In recent years, the use of near field communication (NFC) has expanded, particularly in applications using mobile phones. NFC is an interactive communications technology whose operating principle is based on the proximity contactless communication described above. It has three different modes, which are selected according to their use cases:

- card emulation mode (behaving like an IC card (IC: integrated circuit))
- reader/writer mode (behaving like a reader/writer)
- P2P (peer-to-peer) mode (behaving like transceivers between terminals)

1.2 Potential applications of proximity contactless communication

Proximity contactless communication has a unique feature as a human interface device. By passing a card over a reader/writer, the user is able to access the card's services. Conventionally, the use cases of proximity contactless communication have consisted of using a contactless card and a reader/writer. Recently, however, smartphones and tablet terminals have come equipped with proximity contactless technology that enables them to be used to access a wide variety of services.

New applications will follow these conventional applications (i.e., authentication and payment using contactless IC cards). For example, access to websites related to IC card data and configuration of wireless local area networks and Bluetooth are expected to become easier by passing a terminal in close proximity to an object (such as an IC card and a printer).

2. Overview of standardization organizations

An outline of standardization organizations focusing on proximity contactless communication is shown in **Fig. 1**. Specifications regarding proximity contactless communication have been standardized by many organizations. These standardization organizations cooperate with one another by referencing the standards of other organizations and proposing the standards of one organization to other organizations. Organizations that have had an inter-industrial influence on proximity contactless communication are

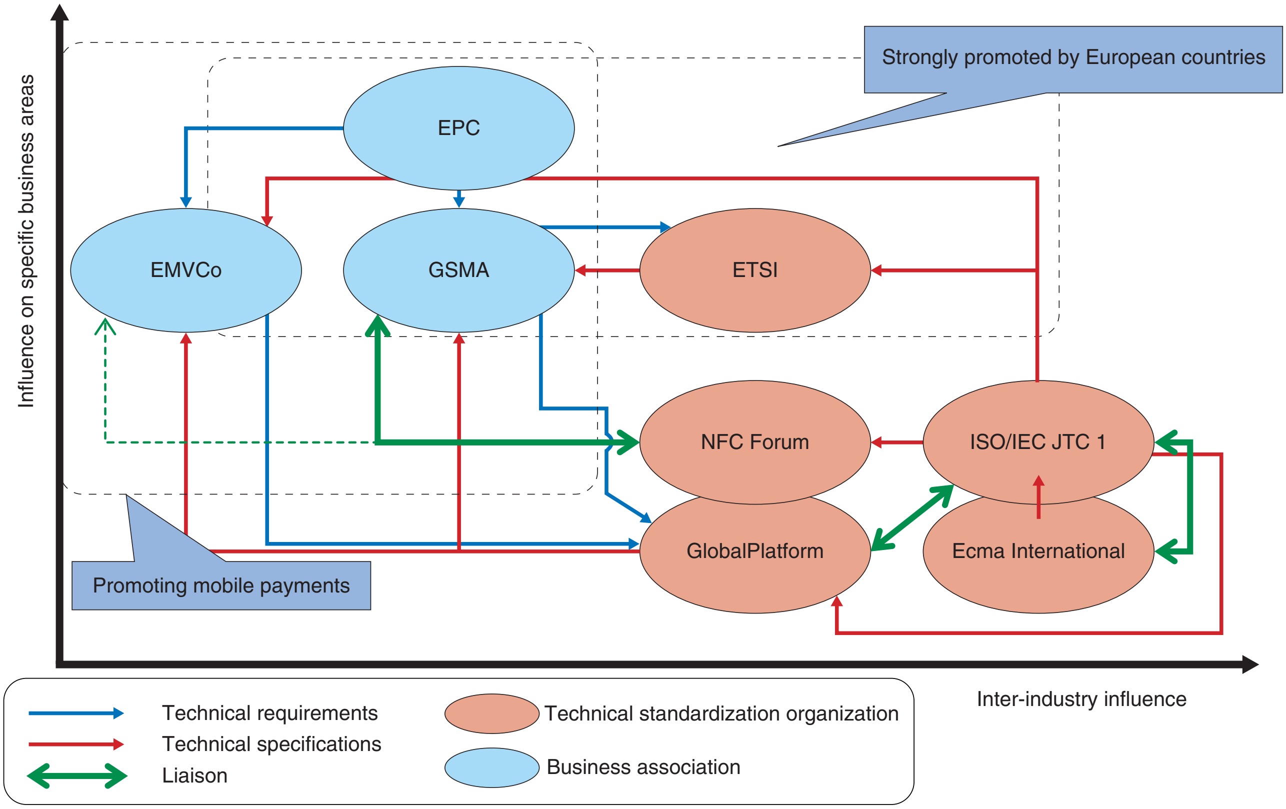

Fig. 1. Overview of standardization organizations.

ISO/IEC JTC 1 (International Organization for Standardization, International Electrotechnical Commission Joint Technical Committee 1), NFC Forum, and GlobalPlatform. Organizations that have had an interbusiness influence on proximity contactless communication are GSMA, EMVCo, and EPC. These organizations liaise with other relevant organizations by proposing standards and exchanging information.

The specifications represented at a lower layer (e.g., RF (radio frequency) interface) are mainly standardized by ISO/IEC JTC1, and those at a higher layer (e.g., platforms and applications) are mainly standardized by GlobalPlatform and NFC Forum.

The group of organizations categorized as business associations (e.g., payment and mobile phone services) establish their standards by referencing existing standards from other organizations and their own specifications.

To develop a system using proximity contactless communication, it is necessary to review the standards established by each organization and to integrate the entire system consistently from the lower to upper layers. Brief descriptions of the organizations are given below. The activities of three of them that are influential to the inter-industry of proximity contactless communication are explained in section 3.

(1) ISO/IEC JTC 1

Extends across ISO and IEC and deliberates on information technology [1], [2].

(2) Ecma International

Deliberates on information and communications technology (ICT) and is a substantial developer of NFC technology [3].

(3) GlobalPlatform

Deliberates on multi-application IC card systems based on open platform technology [4], [5].

(4) NFC Forum

Focuses on NFC technology and products compliant to its specifications [6].

(5) ETSI (European Telecommunications Standards Institute)

Table 1. Standards on contactless interface communication deliberated in ISO/IEC JTC1.

(as of Dec. 2012)

	Title	Version (publication)
Proximity contactless IC card	ISO/IEC 14443-1 Physical Characteristics	2 (June 2008)
	ISO/IEC 14443-2 Radio Frequency Power and Signal Interface	2 (Sep. 2010)
	ISO/IEC 14443-3 Initialization and Anticollision	2 (Apr. 2011)
	ISO/IEC 14443-4 Transmission Protocol	2 (July 2008)
	ISO/IEC 10373-6 Test Methods –Proximity cards	2 (Mar. 2011)
NFC	ISO/IEC 18092 Interface and Protocol (NFCIP-1)	1 (Apr. 2004)
	ISO/IEC 21481 Interface and Protocol -2 (NFCIP-2)	2 (July 2012)
	ISO/IEC 22536 NFCIP-1 RF Interface Test Method	1 (July 2005)
	ISO/IEC 23917 NFCIP-1 Protocol Test Methods	1 (Nov. 2005)
	ISO/IEC 28361 Near Field Communication Wired Interface	1 (Oct. 2007)
	ISO/IEC 13157-1 NFC-SEC: NFCIP-1 Security Services and Protocol	1 (Apr. 2010)
	ISO/IEC 13157-2 NFC-SEC cryptography standard using ECDH and AES	1 (Apr. 2010)

-NFCIP-1: Standard based on the contactless interface of ISO/IEC14443 Type-A and FeliCa (technology developed by Sony)
-NFCIP-2: Standard based on the contactless interface of ISO/IEC 14443 Type-B and ISO/IEC 15693
(Vicinity contactless interface) on top of NFCIP-1
-Wired interface: Digital interface with wired connection between NFC transceiver and NFC front-end
-ECDH: Method of key distribution using elliptic curve cryptography
-AES: New generation cryptography standardized by US National Institute of Standards and Technology

Operates within the EU region focusing on the ICT field [7].

(6) GSMA (Global System for Mobile Communications Association)

Consists of carriers adopting GSM (Global System for Mobile Communications), which presently includes the 3G (third-generation) system [8].

(7) EPC (European Payments Council)

Deliberates on settlement infrastructure [9].

(8) EMVCo

Deliberates on the interoperability of financial services using IC cards and mobile phones; founded by four credit card companies [10].

3. Activities of standardization groups

3.1 ISO/IEC

The technology of contactless IC cards and NFC is categorized as information technology, so JTC1 leads the international standardization in that field [11].

Within ISO/IEC JTC1, 18 subcommittees (SCs) have been formed. Matters related to IC cards and to NFC are respectively handled by SC17 and SC6. Their international standard specifications are listed in **Table 1**.

The first editions of ISO standards for proximity contactless IC cards (ISO/IEC 14443 series) were enacted in 2001. The first edition of ISO standards for NFC (ISO/IEC 18092) was enacted in 2004 and was based on the communication methods used in both Europe and Japan. The coexistence and selection of ISO/IEC 18092 and ISO/IEC 14443 were then standardized as ISO/IEC 21481.

Table 2. Standards deliberated in NFC Forum.

(as of Dec. 2012)

	Title	Outline	Version (publication)
Application layer	NFC Data Exchange Format (NDEF)	Data format for NFC application	1.0 (July 2006)
	NFC Record Type Definition (RTD)	Record used in NDEF	1.0 (July 2006)
	Text Record Type Definition	Record used for displaying text message	1.0 (July 2006)
	URI Record Type Definition	Record used for Web-to services	1.0 (July 2006)
	Signature Record Type Definition	Record for signature	1.0 (Oct. 2009)
	Smart Poster Record Type Definition	Record for smart poster	1.0 (July 2006)
	Generic Control Record Type Definition	Record of implementing multiple functions	1.0 (Mar. 2008)
	Type 1 Tag Operation Specification	Access to NDEF data using TOPAZ	1.1 (Apr. 2011)
	Type 2 Tag Operation Specification	Access to NDEF data using MIFARE Ultralight	1.1 (May 2011)
	Type 3 Tag Operation Specification	Access to NDEF data using FeliCa	1.1 (June 2011)
	Type 4 Tag Operation Specification	Access to NDEF data using products compliant ISO/IEC 14443-4(transmission protocol) and ISO/IEC 7816-4(APDU)	2.0 (Nov. 2010)
Handover	Connection Handover	Selection on wireless interface	1.2 (July 2010)
	Bluetooth Secure Simple Pairing Using NFC	Handover NFC to Bluetooth	1.0 (Oct. 2011)
P2P	Logical Link Control Protocol (LLCP)	NFC Forum specific protocol	1.1 (June 2011)
	Simple NDEF Exchange Protocol	Transmission protocol over LLCP	1.0 (Aug. 2011)
Subset of ISO	NFC Digital Protocol	Subset of ISO/IEC 14443 series and NFC relevant standard	1.0 (Apr. 2009)
Others	NFC Activity Specification	API of NFC firmware	1.0 (Nov. 2010)
	NFC Analog Specification	Analog interface of NFC devices	1.0 (July 2012)

-TOPAZ: Product of Innovision Research & Technology, compliant with ISO/IEC 14443 Type-A
-MIFARE Ultralight: Product of NXP semiconductors, compliant with ISO/IEC 14443 Type-A
-FeliCa: Product of Sony, compliant with ISO/IEC 18092
-APDU: application data unit

ISO/IEC periodically reviews the established international standards. The conventional international standards of proximity contactless IC cards and NFC are currently undergoing revision. The relevant technologies are described below.

(1) Very high bit rate (VHBR)

It is important to implement high-speed data communication in systems that use IC cards containing large amounts of data. The bitrates specified in the ISO/IEC 14443 series are from 106 kbit/s to 848 kbit/s. Specifications for bitrates from 1.70 Mbit/s to 6.78 Mbit/s have been established as amendments for the ISO/IEC14443 series and were enacted in 2012.

(2) Proximity extended device (PXD)

At the time of enactment of the first edition of the ISO/IEC 14443 series, there was an assumption that the functions of contactless IC cards and their reader/writer were separated. Innovations in electronic device technology have enabled portable terminals to implement the functions of contactless IC cards and their reader/writer within them. The need to use both functions with a single portable device has been increasing, and the method of switching between these functions is under development as an amendment to the ISO/IEC14443 series.

3.2 NFC Forum

NFC Forum mainly specifies application layers and their implementation, which are not specified in ISO/IEC. The public specifications of NFC Forum are listed in **Table 2**. NFC Forum defines the functions of the three modes mentioned previously in combination with the three kinds of contactless interfaces (ISO/IEC14443 Type-A, Type-B, and FeliCa), which is called *mode switching*.

Since 2010, the program called N-Mark has been underway, where the devices are certified for NFC Forum compliance.

NDEF (NFC Data Exchange Format) and RTD (NFC Record Type Definition) are the key formats

Table 3. Standards on contactless interface communication deliberated in GlobalPlatform.

(as of Dec. 2012)

	Title		Outline	Version (publication)
Card	Card Specification		Command and security specification in GP compliant multi-application card	2.2.1 (Jan. 2011)
		Amendment C-Contactless Services	Service specification in GP compliant multi-application card	1.0.1(Feb. 2012)
Device	Secure Element Access Control		Method for upper device to access secure element	1.0 (May 2012)
System	System Messaging Specification for Management of Mobile-NFC Services		Message and profile in mobile-NFC services	1.0 (Feb. 2011)

Secure element: Semiconductor designated as tamper-proof that is equipped with secured memory and cryptography. It is implemented using a SIM card embedded in the device.

specified in NFC Forum. NDEF is a data format for NFC applications. RTD is the format for NDEF records specified for each type of application. These specifications enable access to websites, NFC smartphone displays, electronic signatures, and other capabilities, which makes it possible to achieve a variety of services using NFC-enabled smartphones.

3.3 GlobalPlatform

GlobalPlatform (GP) is developing and deploying standards with a focus on the management of IC card applications for various fields from an industry-neutral standpoint.

Card specifications developed by GP have been adopted for SIM (subscriber identity module) cards and are a de facto standard of application management in the field of mobile communication. Furthermore, the test specifications are defined through a conformance testing certification process that exists at GP.

In recent years, GP has been working on standardization for the management of devices with a proximity contactless interface. The GP standards related to the proximity contactless interface are listed in **Table 3**. GP standards will have a stronger influence on the services using proximity contactless cards and NFC-enabled smartphones.

NTT has greatly contributed to GP activities through its staff serving on GP's board of directors and by hosting GP conferences and seminars.

One of the most remarkable specifications recently deliberated at GP concerned multi-secure elements (SEs). This is a method for managing multiple SEs installed in mobile phones from remote servers. This enables services involving the collaboration of multiple applications in the mobile phone (e.g., e-money charging with the user's ID (identity) in the SIM and an e-money application in the embedded device in the phone).

4. Future trends and NTT's involvement

With the spread of mobile devices represented by NFC-enabled smartphones, the use cases of proximity contactless devices will be expanded. Furthermore, SIMs, which are conventionally used only for subscriber identification, are expected to be used for new services in which an application program is downloaded into the vacant memory in a SIM. Thus, it is assumed that the standardization for the upper layer will be accelerated, which will lead to greater utilization of the established contactless proximity communication technology and secure devices.

Through participation in these kinds of standardization activities, NTT is working to achieve an information infrastructure that is both open and interoperable to allow anyone the carefree, secure, and easy use of ICT services anywhere in the world.

References

[1] ISO. http://www.iso.org/iso/home.html

[2] IEC. http://www.iec.ch/

[3] ECMA. http://www.ecma-international.org/

[4] E. Niwano and H. Goromaru, "Standardization Trends at GlobalPlatform," NTT Technical Review, Vol. 4, No. 11, pp. 48–52, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200611048.pdf

[5] GlobalPlatform. http://www.globalplatform.org

[6] NFC Forum. http://www.nfc-forum.org/

[7] ETSI. http://www.etsi.org/

[8] GSMA. http://www.gsma.com/

[9] European Payments Council.

http://www.europeanpaymentscouncil.eu/

[10] EMVCo. http://www.emvco.com/

[11] H. Yamamoto, H. Goromaru, M. Ikeda, and E. Niwano, “Trends in ISO/IEC Standardization of IC Card Technology,” NTT Technical Review, Vol. 5, No. 6, 2007.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200706gls.html

Hideaki Yamamoto

Research Engineer, Public ICT Solution Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in electronic engineering from Osaka University in 1994 and 1996, respectively. He has been registered as a Professional Engineer, Japan, in electrical and electronic engineering since 2011. He joined NTT in 1996 and engaged in R&D of wireless card systems. In 1999, he moved to NTT WEST, where he developed new services using contactless IC card payphones. In 2003, he moved to NTT R&D laboratories, where he has been involved in R&D of contactless smart card systems and international standardization of smart cards. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is Vice Chairperson of Standard Assembly T60 (Task force for wireless card systems) in the Association of Radio Industries and Businesses of Japan and is a member of the Japanese National Committee of ISO/IEC SC17 (smart cards). He received FY 2011 Industrial Standardization Awards from the Ministry of Economy, Trade and Industry for his outstanding contributions to activities regarding ISO/IEC SC17/WG8 (contactless cards). He is a member of the Institute of Electronics, Information and Communication Engineers, the Japan Society of Applied Physics, and the Institution of Professional Engineers, Japan.

Kimihiro Yamakoshi

Senior Research Engineer, Public ICT Solution Project, NTT Secure Platform Laboratories.

He received the B.E. degree in physics from Waseda University, Tokyo, and the M.E. degree in physics from Tokyo Institute of Technology in 1988 and 1990, respectively. He joined NTT in 1990 and engaged in R&D of LSI circuit design. In 2004, he moved to NTT Cyber Communications Laboratory Group where he researched IC-card security technology including measures against side-channel attacks, He transferred to NTT Microsystem Integration Laboratories in 2007 and engaged in R&D of low-power wireless ubiquitous terminals. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is currently investigating a secure device system for IC cards and smartphones. He is a member of the committee of the side-channel security WG of Cryptography Research and Evaluation Committees, Japan.

Tetsushi Morita

Senior Research Engineer, Public ICT Solution Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees from Kyoto University in 1996 and 1998, respectively and the Ph.D. degree from Tsukuba University, Ibaraki, in 2010. Since joining NTT Software Laboratories in 1998, he has been engaged in research on an information retrieval and personalization system. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. His current research interests include information technology for public ICT. He is a member of the Information Processing Society of Japan.