Type A/B GP TSM

Technology Reports

Advances with Osaifu-Keitai —Starting Services Supporting NFC (Type A/B) on NTT DOCOMO UIM Cards—

*The Osaifu-Keitai service currently being provided in Japan is based on the FeliCa®*1 mobile contactless IC card service. On the other hand, services using NFC (Type A/B) are expanding outside of Japan, and these are rapidly being adapted to mobile. Accordingly, we have built a server called a TSM, which manages starting of newly developed services that use Type A/B NFC, added to the current Osaifu-Keitai system. This implements the New Osaifu-Keitai system supporting NFC and allowing both systems to be used. In this article, we give an overview of the functions used to manage starting of these services.*

Frontier Services Department

Toshihiro Sugano

Masahiro Shionoiri†

Masataka Kikawa

1. Introduction

For approximately the last eight years, NTT DOCOMO has taken a global lead in providing a commercial mobile service using contactless IC cards, offering our Osaifu-Keitai service in Japan, based on the FeliCa contactless IC card service. As a result, we have achieved market penetration unprecedented in the world, with approximately 35 million users as of the end of July, 2012.

In contrast, services are spreading rapidly outside of Japan using Near Field Communication (NFC)*2 Type A/B*3, an international specification for contactless IC cards that is being adopted quickly. Full-scale commercial mobile services using this technology are being established quickly.

Type A/B is also being used in Japan for services such as driver's licenses, Taspo, and the Basic Resident Register, and such services are gradually increasing.

As described above, services (and infrastructure) supporting FeliCa are already established in Japan, so an environment in which these FeliCa-based services can continue to be used had to be maintained while adding services (and infrastructure) for Type A/B services that can expand into global markets.

We were able to implement the New Osaifu-Keitai service, which allows use of both FeliCa and Type A/B, by implementing mobile terminals equipped for both FeliCa and Type A/B, and building a Trusted Service Manager (TSM)*4 system to manage starting of services. These enable users to use Osaifu-Keitai both within and outside of Japan.

† Currently, New Business Promotion Dept., NEC Inc.

*1 **FeliCa®**: A contactless IC card technology developed by Sony Corp. A registered trademark of Sony Corp.

*2 **NFC**: A short-range wireless communications standard using the 13.56 MHz band and initiated by NXP Semiconductors Inc. and Sony Corp. Provides unified support for FeliCa, Mifare, Type A/B (ISO14443, see *3), and IC tags (ISO/IEC 15693).

In this article, we give an overview of the new Osaifu-Keitai and service starting management function, focusing on the TSM functions.

2. Overview of Contactless IC Card Services

2.1 NFC

NFC is an international standard for contactless IC card interfaces using short-range wireless communication technology, regulated by the International Organization for Standardization (ISO)[*5]. FeliCa and Type A/B are examples of NFC technologies that can be incorporated into mobile terminals to provide various services.

Mobile terminals with NFC implement the following three main functions.

1) Card Emulation Function

The card emulation function enables functions such as credit cards, e-money or transit passes, usually provided with plastic cards, to be emulated on a mobile terminal.

The current Osaifu-Keitai operates as a card emulation function, enabling services such as iD and JR train passes to be used by holding the mobile terminal over the reader.

Having these functions on a mobile terminal also allows greater convenience with features such as being able to check an e-money balance, or pay for on-line charges from any location.

2) R/W Emulation Function

The R/W emulation function enables the mobile teminal to be used as an NFC read/write terminal. By holding the mobile terminal over an IC card or IC tag, the data in the IC card or tag can be referenced or modified. This can be used for functions such as Web site access, as with Smart Posters[*6], or to see the balance on a pre-paid e-money IC card.

3) Peer-to-Peer (P2P) Function

The P2P function enables data transmission or exchange between mobile terminals supporting NFC or with other devices (PCs, tablets, home appliances, etc. that incorporate an NFC function). This is used for transmitting data such as contacts or photos, as with the Android Beam[*7] function.

2.2 Multi-application Platform for the Card Emulation Function

With contactless IC cards that are plastic cards, a single service is loaded onto each IC card, and overall management of the cards is handled by the Service Provider (SP)[*8], who is the issuer of the card. The services on a card are also normally fixed, so services cannot be added or deleted.

In contrast to plastic cards, we assume that multiple services can be used with mobile terminals having an NFC function, and that users can add or delete services as they desire. The environment that enables this is called the multi-application platform.

Thus, there are multiple issuers, which are the SPs, and a third party (the card administrator) must manage partitioning and allocating of domains to each SP. The role of card administrator is fulfilled by the telecommunication carrier, NTT DOCOMO, which is a Mobile Network Operator (MNO), and each SP manages the service it provides within the domain allocated by the card administrator.

Other roles of the card administrator include managing the memory used by the services installed on the mobile terminal and preventing illegitimate content from being provided (**Figure 1**).

3. System Organization

The telecommunication carrier, which acts as the card administrator, needs a system for managing service domains on the mobile terminal. Management of services on the current Osaifu-Keitai service is done using FeliCa, but we have expanded the infrastructure to support the Type A/B international standard and incorporate accumulated know-how regarding multi-application management platforms.

With Type A/B systems, conformance with GlobalPlatform (GP)[*9],

*3 **Type A/B**: A type of contactless IC card with a communications range of approximately 10 cm, specified by the ISO 14443 international standard. Type A and Type B specify two different communication methods for R/W.

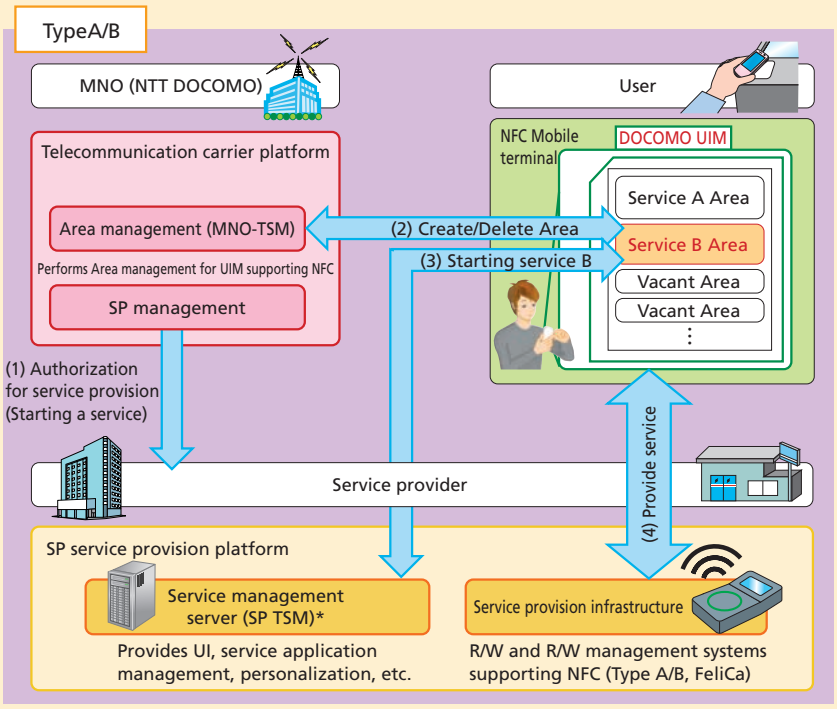
*4 **TSM**: An business entrusted to provide initial start of card applets for UIM cards (See *11) by telecommunication carriers and SPs.

*5 **ISO**: An organization for standardization in the information technology. Sets international standards for all industrial fields except electrical and telecommunication fields.

*6 **Smart Poster**: A type of tag that holds Web addresses and applet information, regulated by the NFC Forum (An organization promoting the spread and creating technical standards for near-field wireless communications).

*7 **Android Beam**: A function for performing data transmission and reception using near-field wireless communications, added starting with Android 4.0.

*8 **SP**: In this article, refers to an operator providing contactless IC card services (NFC services) using the NFC platform.



* For the service management server, ASP functions provided by other companies such as FeliCa Networks can also be used.

Figure 1 Overall organization for providing the Osaifu-Keitai service (supporting NFC)

which was established mainly in the financial industry, is wide-spread.

The organization and role of the system at NTT DOCOMO implementing multi-application and using Type A/B (+GP) technology are shown in **Figure 2**.

3.1 Telecommunication Carrier System Organization

(1) MNO-TSM[*10]

With GP, TSMs accessed through the telecommunication carrier's network are specified in the IC card (the User Identity Module (UIM)[*11]), and one of these is the MNO-TSM, which the telecommunication carrier uses to perform card administration. It performs card administration, creating the Secure Domains (SD)[*12] on the UIM and installing the Applets[*13] needed to provide the SP services.

GP does not specify clearly, the demarcation of responsibilities between the MNO and SPs, but the telecommunication carrier is the domain administrator and the SP is the service provider for the UIM, which belongs to the telecommunication carrier. Accordingly, the telecommunication carrier receives applets belonging to the SPs and registers them using the MNO-TSM.

(2) TSM proxy agent[*14]

GP specifies various formats for communication between the MNO-TSM and the UIM[1], such as HTTP and SMS. HTTP is very compatible with current smartphones, but if HTTP is used the GP specifications recommend using Smart Card Web Server (SCWS)[*15].

There are various concerns with using SCWS, including the impact of implementing it on UIM, and that it cannot be applied to other usage scenarios, so we extracted a part of the SCWS functionality as an Android™[*16] application on the UIM. This allowed us to implement communication between the MNO-TSM and the UIM without using SCWS, while conforming to the interface specified by GP for using HTTP. This Android application is the TSM proxy agent.

The TSM proxy agent fills a proxy roll, executing commands on the Secure Elements (SE)[*17] in the UIM, without parsing the commands received via HTTP from each TSM.

(3) Type A/B SE

Type A/B SEs are a core part of IC chip security and are domains equipped with functionality to man-

*9 **GP**: An organization that creates standards for managing IC cards from a remote server. Also refers to these standards. Initially applied to IC credit cards but was later expanded to apply to IC cards in general.

*10 **MNO-TSM**: Refers to a TSM that performs processing for the responsibilities of an MNO. Includes creating APSDs, loading service Applets, etc.

*11 **UIM**: A card used to store identification and authentication information for users of a mobile network.

*12 **SD**: A type of card applet. A privileged application for application administration. It is able to install and uninstall content, manage the application hierarchy (tree structure), support encrypted communication, manage encryption keys and other tasks according to its configured permissions.

*13 **Applet**: A JavaCard application running on the UICC (See *25) platform. It is stored in a UICC by writing it when the UICC is created or by downloading from a TSM. Refers to both packages and instances in this article.

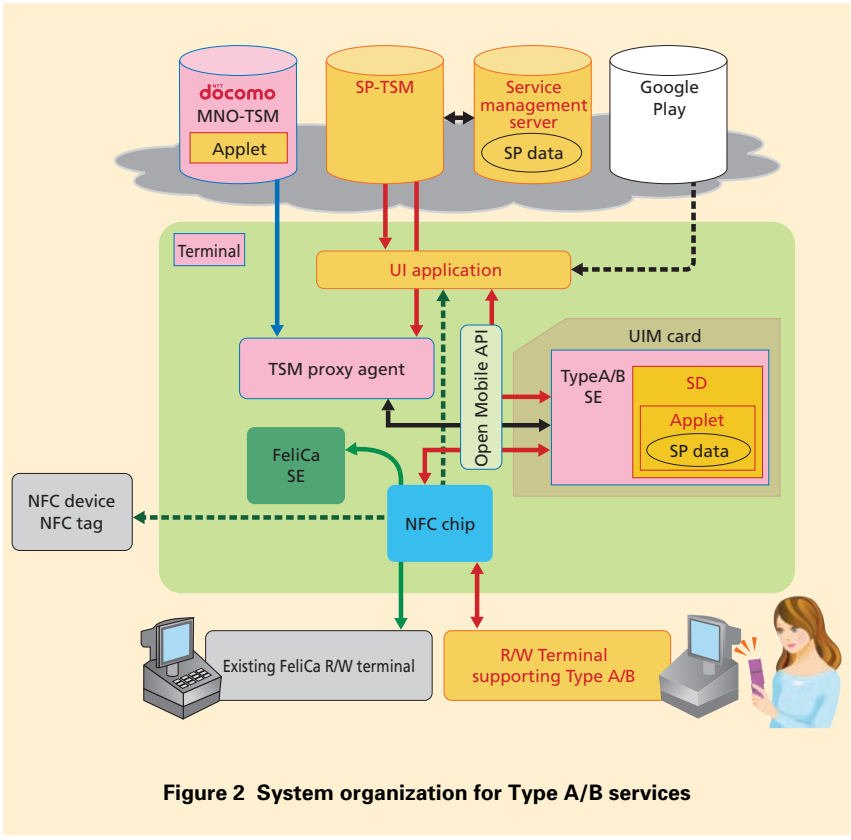


Figure 2 System organization for Type A/B services

age secure data and Applets used by services. NTT DOCOMO implements these Type A/B SE on the UIM, and Applets, which are described below, are stored in these domains.

(4) Terminals (mobile phones)

Here, by terminals, we mean mobile phones incorporating NFC chips that create an environment where Type A/B services can be used.

These terminals also include the middleware[*18] needed to use Type A/B services, such as the TSM proxy agent and the Open Mobile Application Programming Interface (API)[*19].

(5) Service information list display application[*20]

When using multiple services on the multi-application platform, the user needs to be able to check what services have been started in the mobile terminal (UIM). As the card domain administrator, the telecommunication carrier must create a mechanism that can display what is in the SEs in a form viewable by the user. Since, to the users, they are just using Osaifu-Keitai, we make no distinction between FeliCa and Type A/B services, and simply display a list of information regarding the services in each domain.

3.2 SP System Organization

The systems built by SPs include Applets, SP-TSMs[*21], UI applications[*22] and R/W terminals.

(1) Applets

Applet refers to a Java® application[*23] loaded onto the UIM. Applets manage the data on the UIM needed for providing the service, and provide functionality to process commands from the UI applet and R/W terminal. Examples of data managed by an applet include credit card numbers or e-money.

(2) SP-TSM/Service management servers

We refer to the TSMs that perform processing within the responsibility of the SP, such as writing credit card numbers or updating an e-money balance, as SP-TSMs. SPs manage SP data needed to provide their services on a server, and must perform secure communication with an applet stored on the mobile terminal (UIM). The content of this communication is also confidential with respect to the card administrator.

---

*14 **TSM proxy agent**: Controls communication between TSM and SE (See *17). Does not parse the commands it sends to the SE, but acts as a proxy, executing commands received from the TSM in HTTP directly on the UICC (SE).

*15 **SCWS**: A standard platform operating as a Web server in the UIM and managing content remotely.

*16 **Android™**: A trademark or registered trademark of Google, Inc., in the United States.

*17 **SE**: The core part of an IC chip, including security, which is the area used to store value that must be managed securely, such as e-money or credit-card numbers. In some cases, this role is handled by a UICC, but in other cases a chip is built into a mobile terminal or incorporated into an external memory card.

*18 **Middleware**: Software positioned between the OS and user applications, providing functions that are common to multiple applications, thereby making application development more efficient.

*19 **Open Mobile API**: An API specified by the SIMalliance, including APIs for accessing the secure area on a UIM from a UI application or the base terminal software platform.

(3) UI Applications

UI application refers to an Android application distributed to users by the SP, providing the user interface necessary to implement the IC card service. Users can install these applications on their mobile terminals through Google Play™[*24] or dmarket.

Also, when services using an SE domain on a UIM are registered and used, commands are sent from the MNO-TSM or SP-TSM to the Universal Integrated Circuit Card (UICC)[*25] by sending processing requests to the TSM proxy agent from a UI application. There are also use-cases when a UI application reads information written by the applet, such as when displaying an e-money balance[2][3].

(4) R/W Terminal

To provide services, mobile terminals are held over a R/W terminal to allow it to read and write SP data written by an Applet stored in the UIM. More specifically, data such as credit-card numbers or e-money data are read and written to make transactions at a point of sale.

4. Flow/Processing Sequences

4.1 Service Starting

Installation of a service that a user wants to use is called service starting.

To start a service, the user first installs the SP's UI application. Then, to configure the service in a usable state, the corresponding mobile NFC service[*26] applet is installed from the MNO-TSM and user-specific data from the SP-TSM is written (personalization) through operations in that UI application (**Figure 3**). Currently, installation is the responsibility of the telecommunication carrier, and personalization from the SP-TSM is the responsibility of the SP.

4.2 Applet Access

After the service it is started, the data written in the Applet may need to be updated as the user uses it through UI application operations and other means. For example, for an e-money service, this occurs when a charge is processed. In such cases, when the applet data needs to be updated from the SP-TSM, the process is performed through the TSM proxy agent (**Figure 4**).

4.3 Service Deletion

When a user stops using an SP service, such as cancelling a card, they must first terminate the service through the SP UI application or other means, and then the data related to the service (Applet, SD, etc.) must be deleted from the mobile terminal (UIM). When a user deletes a service that has been started on a mobile terminal, it is called service deletion. The user uses operations in the SP UI application to request the MNO-TSM to uninstall the applica-

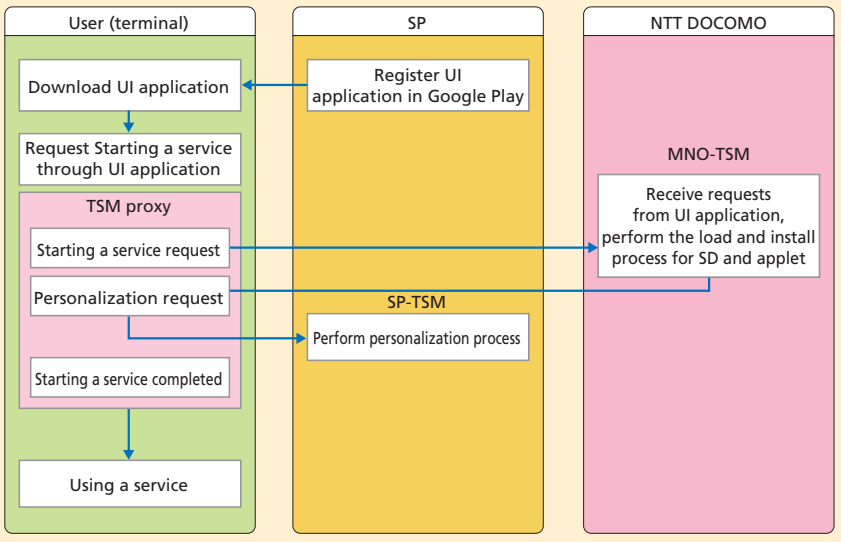


Figure 3 Service starting process

*20 **Service information list display application**: An Android application that displays both FeliCa applications and GP applications in a list.

*21 **SP-TSM**: A TSM that performs processing within the responsibilities of an SP. One such process is service personalization.

*22 **UI Application**: An application that runs on the mobile device, providing an interface for the user. On Android terminals in particular, it is a Java application (See *23).

*23 **Java® application**: A program created using the Java language that runs independently of a Web browser. Different from a Java Applet, it is able to read and write files stored in local memory. Note that Android applications are programmed using Java and run on the Linux kernel. Oracle and Java are registered trademarks of Oracle Corp., its subsidiaries, or related companies in the U.S.A. and other countries. Company and product names appearing in the text may be trademarks or registered trademarks of the respective companies.

ble service applet. Note that depending on the SP service, other processing to delete the service may be required (**Figure 5**).

4.4 SP Authentication

The processing of requests to start, use and delete services as described above is very important and can have a great consequences from the perspective of service operation, so it must not be falsified or impersonated. To prevent such occurrences, the SP is authenticated for all important processes within the responsibility of the telecommunication carrier to ensure they are legitimate, for each request from a UI application or from the SP-TSM.

NTT DOCOMO provides an SP authentication mechanism with a signature[*27] scheme that uses parameters of the processing request. The SP can also decide whether to use static parameters for the signer or to generate them dynamically, so the environment allows for implementation according to the SP's security policy.

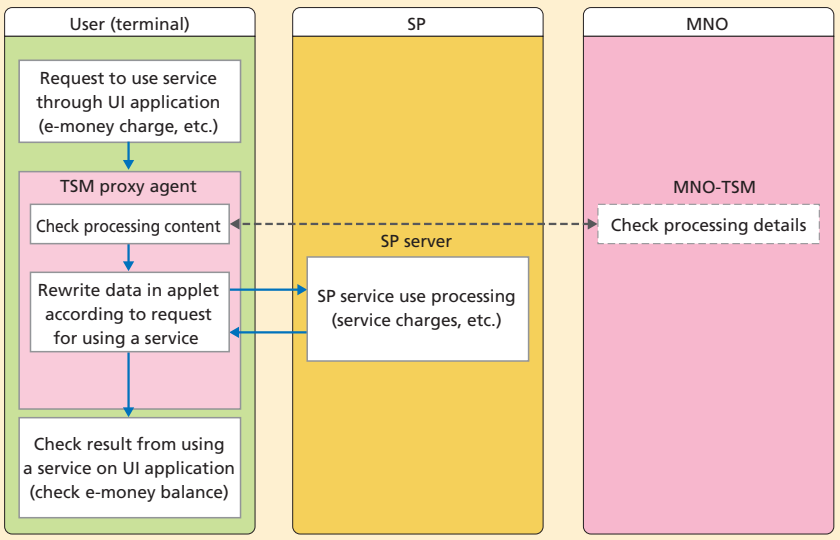


Figure 4 Service use process

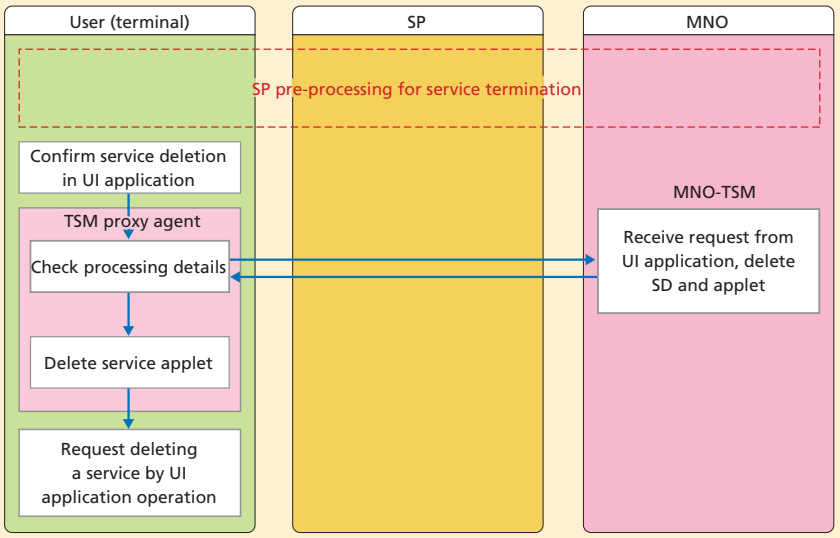


Figure 5 Service deletion process

5. Consortium for Standardizing Specifications

The MNO-TSM and TSM proxy agent described in Chapter 3 conform to GP specifications. However, the division of responsibilities between the SP and telecommunication carrier for the detailed implementation is not clearly specified in the GP specifications, so it is likely that differences will arise in specifications from multiple telecommunication carriers. SPs have also built many systems to provide services, and such differences in telecommunication carrier specifications increase the devel-

*24 **Google Play™**: A service from Google for delivering applications, video, music and books to Android terminals. Google Play™ is a trademark or registered trademark of Google, Inc. U.S.A.

*25 **UICC**: An IC card used to record a unique ID for specifying a phone number. UIM card and SIM card are used synonymously.

*26 **Mobile NFC service**: An NFC service that presumes use of an application stored in a UICC or a mobile device supporting NFC. In this article, NFC service refers mainly to services using infrastructure (readers) for IC cards supporting NFC.

*27 **Signature**: A digital signature required when distributing Android applications, certifying the developer of the application.

opment burden for SPs, which is expected to hinder the spread of services.

Because of this, the three domestic telecommunication carriers in Japan have established the Japan Mobile NFC Consortium, to create common technical and operational specifications for SPs and take measures to expand the spread of these services.

6. Conclusion

The expansion of services supporting Type A/B technology in the future will enable travelers to use mobile credit card services conforming to EMV standards[*28], such as PayPass™[*29] and payWave[*30], and services offered by overseas providers, such as e-money, coupons and transit services.

Also, NTT DOCOMO has built infrastructure with our multi-application platform, and we will contribute to increasing convenience for users by providing new services using this platform.

REFERENCES

[1] GlobalPlatform: "Remote Application Management over HTTP, Card specification V2.2, Amendment B, V1.1," Jun. 2009.
[2] ETSI TS 102 622: "Smart Cards; UICC _Contactless Front-end (CLF) Interface; Host Controller Interface (HCI). v9.3.0," Mar. 2011.
[3] Sun Microsystems, Inc.: "Java Card 3.0.1 Application Programming Interface," May. 2009.

*28 **EMV standard**: A unified specification for IC card readers and an IC credit card terminal that has a defined procedure to perform transactions for both magnetic-strip and IC cards, intended to ease the smooth transition from magnetic-strip cards to IC cards. The standard is oriented to the financial industry and is the standard specification for debit and credit cards.

*29 **PayPass™**: MasterCard's contactless settlement service. PayPass™ is a registered trademark of Master Card International Incorporated.

*30 **payWave**: VISA's contactless settlement service.