mobey forum
mobile financial services

Mobile Financial Services

Terms Explained

Published by Mobey Forum

Document Information

The following organisations have reviewed and contributed to this paper:

EPC – European Payments Council

GSMA

NFC Forum

Smart Card Association

Table of Contents

1. Why is this paper important?

When two powerful and established industries, in this case mobile and finance, start working together, they may see the world from different perspectives and don't necessarily understand each others' jargon. This simple fact may cause misunderstandings and obstacles in the path to successful creation of a new industry.

Mobey Forum has gathered the key terms from financial and telecom industries and aims to harmonize the understanding of these terms, educating the financial industry of the telecoms terms, the telecoms industry of the financial terms and defining the new terms that fall in-between. It is essential for the development of this industry that the relevant terms have the same meaning for everyone.

This document aims to provide the mobile financial services (MFS) industry – its managers, practitioners, the media and consumers – a centralised resource that defines and explains terms relevant to the sector. This is by no means a final or comprehensive list, but rather a living document, where new terms may be added and existing definitions modified as the MFS industry develops and adopts new terminology.

Mobey Forum's paper "Mobile Financial Terms" has been produced by Mobey Forum's members. In a bid to elevate the accuracy and quality of the descriptions offered in the paper, Mobey Forum has engaged with a variety of independent associations in order to obtain their review and input on terms relating to their specialist fields. These associations include, but are not limited to, the European Payments Council, GlobalPlatform, GSMA, NFC Forum and the Smart Card Alliance.

2. Terms from the Mobile Industry

Term	Description
2G	Second generation (2G) is the generic term for the generation of mobile networks that were the first to use packet-based data transmission instead of dial-up connections to enable a data connection. 2G saw the introduction of GPRS and the later increase in speed that was achieved through a technology called EDGE (seen as 2.5G). Further information: CDG, GSMA, ETSI
3G	Third generation (3G) is the generic term used for the third generation of mobile communications systems. These have been created to support the effective over-the-air delivery of a range of multimedia services. On GSM mobile networks the 3G technology is also referred to as Universal Mobile Telecommunications System (UMTS), while the equivalent 3G system on CDMA networks is called CDMA2000. Further information: CDG, GSMA, ETSI, 3GPP
4G	Fourth generation (4G) is the generic term used for the fourth, and at the time of publication latest, generation of mobile communications systems. The major difference is the large increase in the maximum data transmission speeds with download rates of up to 100Mbps and upload rates of up to 50Mbps. For the first time the technology carries the same name across GSM and CDMA networks; it is called LTE (Long Term Evolution). Different countries and mobile network operators use LTE across different frequency bands, including those traditionally associated with previous generations of the mobile telecommunications systems. Further information: CDG, ETSI, 3GPP
Average Revenue Per User (ARPU)	Average Revenue Per User (ARPU) is a common term to measure the impact of promotions, tariff changes, as well as service changes or additions on the revenue of users.

Code Division Multiple Access (CDMA)	Alongside GSM, CDMA (Code Division Multiple Access) is one of the two fundamental mobile telecommunications network technologies. Mobile networks in Asia, the Americas, and Africa use this technology. The technology is driven by the organisation 3GPP. Further information: CDG, GSMA
Communication layers	The communication layer refers to the bearer technology, which allows a transaction to be carried out. The technology through which the transaction is completed can be SMS, IVR, USSD, mobile web or a mobile application dedicated specifically for this purpose. Further information: CDG, GSMA, ETSI
Global System for Mobile communications (GSM)	Alongside CDMA, GSM (Global System for Mobile communications, originally Groupe Speciale Mobile), is one of the two fundamental mobile telecommunications network technologies. Mobile networks across the world use this technology and those in Europe do so exclusively. The technology is driven by several bodies, a major one being ETSI. The more strategic interests of the GSM mobile network operators are represented by the GSMA. Further information: CDG, GSMA
International Mobile Equipment Identity (IMEI)	International Mobile Equipment Identity (IMEI) is the unique serial number of a mobile device. It is used to track down lost or stolen devices. On most devices (excluding iPhones and BlackBerrys) it can be shown by entering *06# as if it was a mobile number and pressing the button to dial this number. Further information: GSMA
Interactive Voice Response (IVR)	Interactive Voice Response (IVR) is used for automated call handling. Companies use IVR e.g. for inbound calls to take automated payments or route callers to the right department, in outbound call scenarios companies use IVR e.g. for fraud prevention calls to verify transactions with customers. Further information: GSMA
Location Based Services (LBS)	Location Based Services use location data either from a GPS radio in the mobile device or from data from the mobile network. Such services can help customers find their way to stores and branches, enable social location services, and enable the context-sensitive delivery of information. Further information: GSMA

Mobile Device	A mobile device is a device with mobile communication capabilities such as a telecom network connection, Wi-Fi and Bluetooth that offer a connection to the internet or other communications networks. Examples of mobile devices include mobile phones, smart phones and tablets.
Mobile (Virtual) Network Operator (MNO/MVNO)	A mobile network operator (MNO) or carrier owns its equipment and offers mobile communication services to its customers. While an MNO often owns its network infrastructure and licensed radio spectrum, a mobile virtual network operator (MVNO) usually does not. An MVNO typically has a business relationship with a larger MNO. An MVNO pays wholesale fees for communication services and then sells the minutes at retail prices under its own brand.
Mobile Application (Mobile App)	Native applications are those that are developed to be downloaded and run on a specific range of mobile devices, while mobile web applications use the device's browser. Native applications can interface with most relevant hardware features of the mobile device, but mobile web applications have very limited ability to do so.
Mobile Identification Number (MIN)	The mobile identification number is the unique number that a mobile network operator uses to identify a SIM. While a subscriber's phone number can change over time with number portability, the MIN always stays the same.
MSISDN	Commonly called MSISDN, the Mobile Station Integrated Services Digital Network is the mobile phone number allocated to a subscriber, commonly known as the phone number. It is used for routing calls to the subscriber. The MSISDN can change over time with number portability (while the MIN identifying the SIM does not change). Further information: GSMA

SIM Card	Commonly called SIM Card, the Subscriber Identity Module Card is a smart card chip used in GSM devices to provide access to the services provided by a mobile network. Access to a SIM card is protected with a PIN and can offer SIM Toolkit services. The SIM Card has a unique fixed number, and a mobile phone number assigned to it by the network operator. Since the introduction of 3G (UMTS) services, the SIM Card is often referred to as USIM (Universal SIM) or UICC (Universal Integrated Circuit Card). In the context of NFC-based services, the SIM card can act as the Secure Element (SE), although other SE options are available. Further information: ETSI
SIM Toolkit (STK)	The SIM Toolkit is a development environment for applications on the SIM Card/UICC. Thus applications are subject to control by the Mobile Network Operator. SIM Toolkit applications can take many forms. Many such applications include text-based menus to make certain functions, such as querying the remaining prepaid balance available, simpler for the user. In Mobile Financial Services SIM Toolkit applications are often used for the menus of mobile money services that communicate with the service via SMS or USSD. Further information: ETSI
Short Message Service (SMS)	Commonly called SMS, the Short Messages Service was originally only meant for communication between GSM network engineers and only later its potential for mobile subscribers was realised. SMS messages are always sent through the SMSC (the Short Message Service Center) of the subscirber's mobile network operator . SMS was not a feature of CDMA networks originally but was later added. In some cases interoperability between GSM and CDMA networks is still not flawless, resulting in delayed or double delivery of messages. Further information: GSMA, CDG, ETSI, 3GPP
UICC Universal SIM (USIM)	Please see the definitions for 'SIM Card' and 'Secure Element'.

Unstructured Supplementary Service Data (USSD)	Unstructured Supplementary Service Data (USSD) is generally associated with real-time or instant messaging type mobile services. It has no store or forward capability that is typical of normal short messages (SMS). This increases the level of security it offers compared to SMS based financial services. USSD does not have roaming capabilities, so it is not suitable for international money transfers. USSD is used via codes that aren't very user-friendly (e.g. *06# to show the mobile device's serial number), so USSD services are often coupled with a text-based menu in a SIM Toolkit application. Further information: GSMA

3. Terms from the finance, banking and payments industry

Term	Definition
Automated Clearing House (ACH)	Automated Clearing House is an electronic network for financial transactions. ACH processes large volumes of credit and debit transactions, usually in batches. ACH credit transfers include direct deposit payroll and vendor payments. ACH direct debit includes the collections of insurance premiums, mortgage loans, and other bills.
Acquirer (merchant/consumer)	An acquirer is a payment service provider that enables the processing of a merchant's transaction with the issuer through an authorisation and clearing network. In the context of mobile financial services it effectively means the entity that accepts mobile payments. From BIS: An Acquirer is the entity or entities that hold(s) deposit accounts for card acceptors (merchants) and to which the card acceptor transmits the data relating to the transaction. The acquirer is responsible for the collection of transaction information and settlement with the acceptors. Further information: BIS
Anti-Money Laundering (AML)	Anti-Money Laundering refers to the legal controls that are required from financial institutions and other regulated entities to prevent, detect and report money laundering activities. Further information: World Bank
Bank Identification Number (BIN)	Usually the first six digits of a credit card number are referred to as the Bank Identification Number. BIN is a code that uniquely identifies a bank and possibly a branch as part of a financial institution. The term Issuer Identification Number (IIN) supersedes the term BIN. ISO/IEC 7812-1 specifies the numbering system for the identification of issuers of identification cards used in international and/or inter-industry interchange.
Business Identifier Code (BIC)	The business identifier code is series of codes developed by the International Organization for Standardization (ISO), standard 9362, and are used to identify banks and their branches in financial transactions. The BIC is either eight or 11 digits long. An eight-digit code refers to a primary office of a bank and the 11-digit code refers to a specific branch. The code specifies the bank, the country, the location and the branch. BIC codes are also called SWIFT codes. Further information: ISO

Basic bank account number (BBAN)	The Basic Bank Account Number is a domestic identifier of a specific account and follows a specific standardised length. The BBAN includes the domestic bank account number with branch information, and may also include routing information. The BBAN forms part of the International Bank Account Number (IBAN). Further information: ISO
Central Infrastructure Manager (CIM)	A central infrastructure manager can be used as a centralized directory service to enable mobile remote payments. The directory provider will link a customer's mobile identifier (normally the mobile phone number) to their default payment instrument, such as a credit card or a bank account. This will enable the mobile identifier to act as a proxy for the card or account number to facilitate payments over existing networks. This role can also be fully or partially undertaken by a third party technology provider or a mobile operator. The CIM can also offer and operate customer authentication services.
EMV/EMVCo	EMV is the standard specification for chips-based cards created by Europay, MasterCard and Visa. The aim of the standard is to promote the compatibility of chip-based card payments. EMV part 1 corresponds with (and generally conforms with) ISO 7816 parts 1-5. The other parts of this specification cover the details of a standard credit/debit application and the requirements for terminals. EMVCo is the company behind the EMV standard and also standardised the use of contacless cards as well as use of card accounts with an NFC-capable mobile device. From emvco.com: EMV® is a global standard for credit and debit payment cards based on chip card technology. EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa. Further information: EMVCo, ISO

International Bank Account Number (IBAN)	An expanded version of the Basic Bank Account Number (BBAN) used internationally to uniquely identify the account of a customer at a financial institution. The IBAN is an international standard for identifying bank accounts across national borders with a minimal risk of propagating transcription errors. The standard was adopted by the European Committee for Banking Standards (ECBS), but later adopted as an international standard under ISO 13616:1997. The current standard is ISO 13616:2007, which indicates SWIFT as the formal registrar. IBAN can reach a total length of 34 characters, starting with two-letter ISO country-code, followed by two check-digits, and ending in the BBAN. Further information: ISO
Issuer	An issuer is a company or municipality that offers securities for sale to investors. Examples include corporations, investment trusts, and government entities. In the payments industry however, the issuer is commonly understood to be a financial institution issuing a debit or credit account with a card. From BIS: in a stored value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it. From ECB: a fi nancial institution that makes payment cards available to cardholders, authorises transactions at point-of-sale (POS) terminals or automated teller machines (ATMs) and guarantees payment to the acquirer for transactions that are in conformity with the rules of the relevant scheme.
Issuing bank	An issuing bank is the bank that offers card association branded payment cards directly to consumers. The issuing bank assumes primary liability for the consumer's capacity to pay off debts they incur with their card. Issuing banks are commonly also simply referred to as “issuer”. From BIS: Issuing institution: the institution receiving funds in exchange for value distributed in the system and, in principle, being obliged to pay or redeem the customer’s transactions and unused funds which are presented to it. It is normally the institution which invests the float. Further information: EMVCo

Know Your Customer (KYC)	Know your customer in the financial industry refers to the requirement (by regulation or legislation) of financial institutions to confirm the identity, background and other aspects of the source of funds of potential and existing customers. The aim of these requirements is to prevent and aid combating of money laundering, terrorist financing and financial crime. Further information: World Bank, Payment Services Directive
Key	A key is a string of meaningless bits until it is used to encode or decode a message. In modern encryption systems, the algorithm is generally assumed to be known but the key is secret. EMV Book 2 defines it as the following: 'A sequence of symbols (or bits) that controls the operation of a cryptographic transformation'.
Offline transactions & online transactions	In certain scenarios transactions can be authorised offline, as the transaction is not going through the payment network for authorisation by the issuer. The smart card's chip includes information that makes an offline authorisation possible. An online transaction is a password-protected payment method that authorizes a transfer of funds over an electronic funds transfer. Further information: EMVCo
Omnibus Account	The omnibus account, held by a financial institution, covers the total sum of deposits spread across all stored value accounts that a service provider manages on its system. Further information: ECB (general)
Primary Account Number (PAN)	A Primary Account Number is the 16 to 19 digit long number found on the face of a bank card, as well as in the payment application in the chip. The PAN is defined in ISO 7812. It consists of a six-digit Issuer Identification Number (IIN), an individual account identifier of variable length and a single check digit calculated using the Luhn algorithm. Further information: EMVCo
Payment corridor	A payment corridor defines the route for a remittance money transfer from sender to receiver. These are usually international but can also be for domestic corridors in larger countries.

Payment processor	A payment processor is a company that handles credit, debit and prepaid transactions on behalf of the issuers and the acquieres for the transaction. It processes transactions interbank for the benefit of payers and payees for other payment transactions.
Payee (or Receiver)	The payee is an individual or a business that accepts and receives payments over various channels including mobile channels.
Payer (or Sender)	The payer is an individual that initiates a payment transaction, which is processed through a payment provider. The payment can be initiated over various channels including the mobile channel.
Payment Network	The payment network is an existing payment system, over which payment transactions are completed for example an Automated Clearing House (ACH) or a clearing service for moving funds across bank accounts or payment card networks such as Visa, Amex or MasterCard.
Payment Service Provider	Payment service providers are companies (such as banks, financial institutions or mobile network operators) that hold a license to provide payment services. The official and full definition of Payment Service Providers describes the bodies referred to in Article 1 of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, legal and natural persons benefiting from the waiver under Article 26 of the aforementioned. US-based on-line payment service providers are supervised by the Financial Crimes Enforcement Network (or FinCEN), a bureau of the United States Department of the Treasury that collects and analyzes information about financial transactions in order to combat money laundering, terrorist financiers, and other financial crimes.
Point of Sale (POS)	A point of sale (POS) terminal holds the hardware and software needed to accept payments. The point of sale system manages the selling process with a salesperson-accessible interface. Further information: EMVCo

Single Euro Payments Area (SEPA)	The Single Euro Payments Area (SEPA) stands for the European Union (EU) payments integration initiative. The SEPA vision was set out by EU governments in the Lisbon Agenda, March 2000, which aims to make Europe more dynamic and competitive. Following the introduction of euro notes and coins in 2002, the political drivers of the SEPA initiative - EU governments, the European Commission and the European Central Bank (ECB) - have focused on the integration of the euro payments market. Since then, the political drivers have called upon the payments industry to bolster the common currency, by developing a set of harmonised payment schemes and frameworks for electronic euro payments. Integrating the multitude of existing national euro credit transfer and euro direct debit schemes into a single set of European payment schemes is a natural step towards making the euro a single and fully operational currency. Creating a SEPA for cards aims at ensuring a consistent customer experience when making or accepting payments with cards throughout the euro area. Last but not least, the SEPA programme seeks to incentivise increased use of electronic payment instruments, while reducing the cost of wholesale cash distribution. SEPA currently consists of the EU Member States plus Iceland, Norway, Liechtenstein, Switzerland and Monaco. Within SEPA, bank customers can make electronic euro payments across these countries under the same basic rights and obligations. Further information: EPC, ECB, EC
Tokenisation	Tokenization refers to a process by which a piece of sensitive data, such as a credit card number, is replaced by a surrogate value known as a token. The sensitive data still generally needs to be stored securely at one centralized location for subsequent reference and requires strong protections around it. The security of a tokenization approach depends on the security of the sensitive values and the algorithm and process used to create the surrogate value and map it back to the original value. Source: Gartner

Terms for Different Transaction Types

Term	Description
Business-to-Business (B2B) transactions	B2B transactions are payments or fund transfers between two businesses. These can be payments for goods and services.
Business-to-Person (B2P) transactions	B2P transactions are payments or fund transfers from a business to a person, including but not limited to salary payments.
Government-to-Person (G2P) transactions	G2P transactions are payments or fund transfers from a government body to a person, for example welfare, and other social benefits payments.
Person-to-Business (P2B) transactions	A P2B transaction can be defined as individual person making payments to businesses for physical or digital goods and services.
Person-to-Government (P2G) transactions	P2G transactions are payments or funds transfers from a person to a government body, for example tax payments and levies.
Person-to-Person (P2P) transactions	In the context of mobile financial services, P2P transactions refer to the payment of funds from one individual to another using a mobile device. P2P transactions are also referred to as mobile money transfers (MMT).

4. Terms for Mobile Financial Services

Term	Description
Authentication	The provision of assurance of the claimed entity or of data origin.
Authentication Method	The method used for the authentication of an entity or data origin.
Authenticator	A security factor used in an authentication method. Typical examples are tokens, mobile codes and passcodes.
Dynamic Authentication	An authentication method that uses cryptography or other techniques to create a one-per-transaction authenticator. This dynamic authenticator changes randomly with each transaction.
Static Authentication	An authentication method that always uses the same authenticator.
Strong Authenticator	An authentication method that involves at least two independent authenticators (i.e. something the user knows, possesses or is).
Strong Dynamic Authentication	A dynamic authentication method that involves at least two independent authenticatiors (i.e. something the user knows, possesses or is).
Authentication - One-Way	An exchange of evidence from a first entity to a second entity that provides enough information to the second entity that they believe the first entity is who/what they claim to be. This evidence is usually classified as either: 1) something-you-know such as a password or PIN 2) something-you-have such as a mobile device or smart card and 3) something-you-are such as a fingerprint or other unique biometric identifier. Further information: FFIEC

Authentication – Mutual (Two-Way)	An exchange of evidence as in one-way authentication (explained above), but to both directions: from a first entity to a second entity (One-Way) and back (Two-Way).
Debit Account	An individual account used to make purchases with one's own money. This account type is usually directly provided by a financial institution. The individual account funds all financial transactions.
Prepaid Account	An account funded in some manner prior to transaction use.
Cardless ATM Withdrawal	Instead of the account holder inserting their card into the cash machine, the account holder can obtain a withdrawal code through user preferred interface the bank supports for this process, but in most cases it will involve the mobile device. The account holder then typically enters their mobile number and the withdrawal code in order to obtain the funds.
Credit Account	An account, provided by a financial institution, merchant, or third party, that provides funding and accumulates financial transactions that enables the account holder to purchase goods and services and pay for them later. At some point in time, the account provider and funder requests payment from the account holder. If partial payment is provided, unpaid portions are owed by the account holder to the account provider with agreed additional interest amounts.
Stored Value Account (SVA)	A Stored Value Account is a balance managed on a secure server for a user and commonly a much lighter type of account compared to a full bank account. SVAs often share the characteristics of low balance, low value transactions, and high number of accounts. The funds corresponding to the balances in the SVAs are covered in an omnibus account held by the responsible financial institution.

Mobile Banking (mBanking, m-Banking)	Mobile banking in its simplest form lets a user retrieve the balance of an account, a small number of the recent transactions, and transfer funds in-between accounts that the user holds. In the widest of senses mobile banking is advanced enough to replace the entire suite of service offered through a bank's branch and internet banking services.
Mobile Commerce (mCommerce, m-Commerce)	Mobile Commerce is the delivery of electronic commerce capabilities directly into the consumer´s device, anywhere, anytime via cellular and wireless networks [Global Mobile Commerce Forum]
Mobile Financial Services (MFS)	Mobile financial services is an umbrella term used to describe any financial service that is provided using a mobile device.
Mobile Payments (mPayments, m-Payments)	Mobile Payments are payments for which the data and instruction are initiated, transmitted or confirmed via a mobile device. This can apply to online or offline purchases of services and digital or physical goods as well as P2P payments, including transfer of funds. Mobile payments are often divided into two main categories; proximity payments and remote payments. However, the two are converging as neither is tied to a specific technology.
Mobile POS (mPOS)	A mobile point-of-sale (mPOS) refers to using a consumer mobile device (ie smartphones, tablets) to facilitate payments and enable acceptance of payment instruments such as credit cards, debit cards and/or cash. mPOS devices leverage both hardware and software components to allow a merchant or individual to accept payments. To support the various card reading modalities (magnetic stripe, Chip and NFC/Contactless) some form of add-on physical hardware such as a sleeve, dongle or card reader is typically required.

Mobile Wallet (mWallet, m-Wallet)	Mobile wallet refers to the functionality on a mobile device that can interact securely with digitized valuables. It includes the ability to use a mobile device to conduct commercial transactions in the physical world. A mobile wallet may reside on a mobile device or on a remote network/secure server. Alongside the ability to undertake payments, the Mobile Wallet may contain other content, such as identity, commerce and banking services, transport and other tickets, retail vouchers and loyalty programmes. Further information: Mobey Forum, GSMA
Social location services	Social location services combine social network traits with real-world locations. Users can "check-in" to locations and users following them will get a notification about this. Some services assign points for different actions and show leader boards amongst friends. Businesses are encouraged to claim their venues and use these social location services to track, build and reward loyalty with their customers. Rewards take different forms and could be discounts on purchases or giving the nth product for free.

5. Terms for Mobile Proximity Payments

Term	Description
MIFARE™	MIFARE™ is a trademark of NXP Semiconductors and refers to a series of chips used in contactless smart cards. MIFARE™ has been used in most of the contactless smart card fare collection projects worldwide.
Mobile proximity payment	Mobile proximity payments (in contrast to remote payments) are transactions that require that the payment device (contactless card, token, phone) is in close proximity to a payment terminal. For example, in NFC payments a consumer waves, taps or touches their mobile payment device to communicate with a merchant's point of sale terminal to pay for goods or services. These types of contactless transactions use short-range wireless frequences and do not use the cellular network of a mobile network operator. Currently the most strongly emerging technology standard for proximity payments is near field communication (NFC). This technology brings the feature of contactless cards to mobile devices. Other technologies like Bluetooth, QR, barcodes, infrared or voice recognition can also be used and have the advantage of not requiring an NFC enabled device.

Near Field Communication (NFC)	NFC Forum proposed definition. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and enables a consumer to utilize one device across different systems. Extending the ability of the contactless card technology, NFC also enables devices to share information at a distance less than 4 centimeters with a maximum communication speed of 424kbps. Users can share business cards, make transactions, access information from smart posters or provide credentials for access control systems with a simple touch. NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. For example if the user wants to connect their mobile device to their stereo to play media, they can simply touch the device to the stereo's NFC touch point and the devices will negotiate the best wireless technology to use. Further information: EMVCo, ISO, NFC Forum
NFC enabled device	An NFC-enabled device is a device that is capable of performing near field communication. Source: NFC Forum
NFC Modes	NFC technology includes three modes of operation: • Peer-to-peer mode enables two NFC devices to communicate with each other to exchange information and share files. Users of NFC-enabled devices can quickly share contact information and other files with a touch. • Reader/writer mode enables NFC devices to read information stored on inexpensive NFC tags embedded in smart posters and displays. NFC-enabled devices can access information from embedded tags in smart posters. • Card emulation mode enables NFC devices to act like smart cards, allowing users to perform transactions such as retail purchases and transit access with just a touch. This mode is capable of functioning when the device is powered-off, although it is the service provider's decision whether to allow this. Source: NFC Forum

Over-the-Air (OTA) provisioning	Over-the-air (OTA) provisioning is the ability to download and manage content on a device over a cellular or wireless network. In the context of mobile proximity payments this applies especially to the over-the-air personalisation and life cycle management of a payment instrument in the secure element in a mobile device. This process is commonly executed through the mediation of a Trusted Service Manager (TSM), employing cellular and wireless networks to reach the mobile device.
Point of Interaction (POI)	Point of Interaction is the intitalpoint where data is enterd into the payment system. POI can be physical or virtual, while a POS is always physical. POI can is often used for electronic or mobile commerce.
Secure Element (SE)	A secure element is a platform or a device used to securely store application-critical data (such as secret keys). A secure element will host a number of secure element applications, also known as applets. These applications are often installed, personalised and managed over-the-air. Examples of secure element form factors in mobile devices include UICC (SIM card), embedded SE (eSE) chip cards and (micro) SD cards. Owing to space limitations on the SE of UICC, it is usual to mediate between the end-user and the SE applet through a mobile application (app). In other words, an app is needed to provide the user interface (UI) to the SE applet – although the interaction may be confined to very simple matters such as activation/deactivation. Further information: EMVCo, Global Platform, GSMA
Trusted Execution Environment (TEE)	An execution environment that runs alongside but isolated from an REE (run-time execution environment). A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. Further information: Global Platform

Trusted Service Manager (TSM)	A trusted service manager (TSM) is a role typical in a near field communication ecosystem, where hardware secure element is in use. The trusted service manager acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, mobile device manufacturers or other entities controlling the secure element (SE) on mobile devices. The trusted service manager enables service providers (SPs) to distribute and manage contactless applications remotely by allowing controlled access to the secure element in NFC-enabled handsets. In typical deployments, the TSM role is split in two – the Secure Element Issuer TSM (SEI TSM) and the Service Provider TSM (SP TSM). The Service Provider TSM manages the service provider's application provisioning to the SE and its application lifecycles. The Secure Element Issuer TSM manages secure element lifecycles and security domains on behalf of SPs. The TSM is an independent business entity and many types of company are entering this competitive market. Many payment card manufacturing companies and card personalisation bureaus are already providing TSM services. Mobile Network Operators (MNOs) typically need to establish one or more SEI TSMs to manage their UICC-based secure element (the MNO being the issuer of this SE type). In this case, the SEI TSM may be deployed within each MNO or may be an independent entity serving many MNOs. Note: the terminology 'Issuer' and 'Service Provider' in this context arise from outside the Financial Services industry: 'Issuer' being the Secure Element Issuer, and 'Service Provider' being known in Financial Services as the (payment instrument) issuing bank or simply issuer. Further information: EPC, EMVCo, Mobey Forum, GSMA
Trusted Third Party	A trusted third party is a body that holds keys for authorization processes.

6. Terms for Mobile Remote Payments

This section contains terms commonly used to talk about mobile remote payments.

Term	Description
Mobile Money	Mobile Money is a very general term meaning any financial action made with a mobile device.
Mobile remote payment	A payment intitated by a mobile device where the transaction is conducted over a mobile telecommunications network (e.g. GSM, mobile internet) and which can be made independent of the payer's location (and/or his/her equipment).
Mobile money transfer (MMT)	A Mobile Money Transfer is the exchange of funds from one party to another, using a mobile device to either initiate and/or complete the transaction.
Mobile remittance	A mobile remittance is a mobile money transfer, mostly across international borders. It is considered a separate category of mobile remote payments due to the relatively higher payment value, possible foreign exchange requirement and regulatory complexity.
Mobile Remote Capture (MRC)	The availability of cameras in smartphones has given rise to the ability to capture cheques, bills and other payment related documents remotely instead of having to bring them to a branch. Using a mobile application, the user takes a picture of a document that is analysed buy the MRC software to read out the payment instructions. The instructions are then submitted to the bank for processing. Alternative names for this type of feature are remote deposit capture, or mobile remote deposit.

7. Terms for Mobile Wallet

Term	Description
Mobile Wallet Content	Mobile wallet content refers to the digital content that resides within a mobile device and on secure servers and provides value to the mobile wallet user. The mobile wallet could contain different tradable value including currency and other value such as coupons, loyalty points, credits or virtual currencies. Further mobile wallet content could be identity or banking services, or transport and other tickets.
Mobile Wallet Content Provider	The mobile wallet content providers are the organisations or the brands that issue content for use in the mobile wallet. Outside Financial Services, such a provider might be known as a Service Provider. Within Financial Services, an issuing bank could be an example of a content provider.
Mobile Wallet Control Point	The mobile wallet control points are the essential components of mobile wallet operations that enable a mobile wallet stakeholder to control how a part of the ecosystem operates. Such control points could be internal to the mobile wallet, or external to it relating to the use of the mobile wallet and its content in the world of commerce. Further information: Mobey Forum white paper on mobile wallet control points
Mobile Wallet User	The mobile wallet user is the individual who uses a mobile wallet, manages its content to control their personal data and accesses financial services remotely.
Mobile Wallet Provider	A mobile wallet provider is an organisation or a brand that issues the necessary mobile wallet functionality to the mobile wallet user.
Mobile Wallet Stakeholder	A stakeholder in the mobile wallet ecosystem is any organisation or individual that provides, provisions, or uses mobile wallets and their associated content and ecosystem. The key groups of mobile wallet stakeholders include the mobile wallet content provider, the user and the payment service provider.

8. Other Terms and Definitions

Term	Description
Chip manufacturer	A chip manufacturer is a company that manufactures microchips (tiny slices of semiconducting material on which a transistor or entire integrated circuit is formed).
User Interface (UI)	A user interface is the system by which users interact with a machine. The user interface includes hardware and software components. On a mobile device the software component of a UI is realized though a mobile application (app).
Web Application (Web App)	A Web App, most commonly developed leveraging HTML5, is an app that works similarly across different browsers, both on mobile and desktop computing devices. Financial services that don't require access to a lot of hardware features benefit from being built as a web app, avoiding the need for example to develop native applications for different mobile platforms. Further information: W3C
Responsive Design	Modern web sites these days leverage responsive design to have one site for different devices (mobile, tablet, desktop), with different resolutions and orientations (portrait vs landscape). Responsive design sites automatically change the layout of the site depending on the capabilities and orientation of the accessing devices.Further information: W3C
Service provider	A service provider is the business entity providing the service in question either to end-user or to another business entity. In mobile financial services service provider normally refers to the company providing the technology that enables the service. Outside Financial Services the term Service Provider refers to an entity with which the end-user has a relationship, such a transport provider.

Smart card	A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g. encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443). It is available in a variety of form factors, incl. plastic cards, key fobs, watches, subscriber identification modules used in GSM mobile phones, and USB-based tokens. See also SIM Card. Further information: Smart Card Alliance

9. Industry Stakeholders

3rd Generation Partnership Project (3GPP)

The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies for mobile networks using the GSM standards.

The 3GPP is the GSM technology's equivalent to the CDMA technology's CDG.

For further information please visit: http://www.3gpp.org/

CDMA Development Group (CDG)

The CDMA Development Group, founded in December 1993, is an international consortium of companies who work together to lead the growth and evolution of advanced wireless telecommunication systems based on CDMA technology. The CDG is comprised of service providers, infrastructure manufacturers, device suppliers, test equipment vendors, application developers and content providers.
The CDG is the CDMA technology's equivalent to the GSM technology's 3GPP.

For further information please visit: http://www.cdg.org/

EMVco

EMVCo, owned by American Express, JCB, MasterCard and Visa, manages, maintains and enhances the EMV®1 Integrated Circuit Card Specifications to ensure global interoperability of chip-based payment instruments with acceptance devices including point of sale terminals and ATMs. EMVCo also administers a testing and approval process, and oversees the procedures for confirming compliance with the EMV standards.

For further information please visit www.emvco.com

European Payments Council (EPC)

The European Payments Council (EPC) is the coordination and decision-making body of the European banking industry in relation to payments. The purpose of the EPC is to support and promote the Single Euro Payments Area (SEPA).

The EPC develops payment schemes and frameworks which help to realise the integrated euro payments market. In particular, the EPC defines common positions for the cooperative space of payment services
For further information please visit: http://www.europeanpaymentscouncil.eu/

European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ETIS is officially recognized by the European Union as a European Standards Organization. ETSI is a not-for-profit organization with more than 700 ETSI member organizations drawn from 62 countries across 5 continents world-wide.

For further information please visit: http://www.etsi.org/

Global Platform

GlobalPlatform is a cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology.
Global Platform launched their Mobile Task Force in April 2007 to actively contribute to the development of mobile telecommunications standards worldwide.

For further information please visit: http://www.globalplatform.org/

Government or Regulatory Entities

Government organisations and regulatory bodies aim to have relevant rules and regulations in place that keep payment systems secure and ensure that the interests of consumers and other payment system users are safeguarded and protected.

GSMA

The GSMA represents the interests of mobile telecommunications operators (Mobile Network Operators) worldwide. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. Mobile Network Operators own and manage the SIM Card – the UICC on which the mobile subscription is managed – which is capable of acting as a Secure Element.

For further information please visit: http://www.gsma.com/

Mobey Forum

Mobey Forum is a global, bank-driven business association working to accelerate the evolution and adoption of mobile financial services. Established in 2000, it brings together leading financial institutions, mobile network operators, mobile handset manufacturers and payment processors and vendors, committed to accelerating the mass-market deployment of user-friendly mobile financial services by promoting open and secure technology standards.

For further information please visit: http://www.mobeyforum.org/

NFC Forum

The NFC Forum was launched as a non-profit industry association in 2004 by leading mobile communications, semiconductor, and consumer electronics companies. The Forum's mission is to advance the use of Near Field Communication technology through developing specifications that ensure interoperability across devices and services, and educating stakeholders about NFC technology. The Forum's 180 global member companies currently are developing specifications for a modular NFC device architecture, and protocols for interoperable data exchange and device-independent service delivery, device discovery, and device capability.

The NFC Forum's Board of Directors is made up of Sponsor-level members that include leading players in key industries around the world. These Sponsor members are Broadcom Corporation, INSIDE Secure, Intel, MasterCard Worldwide, NEC, Nokia, NXP Semiconductors, Qualcomm, Renesas Electronics Corporation, Samsung, Sony Corporation, STMicroelectronics, and Visa Inc.

For futher information please visit www.nfc-forum.org

Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

For further information, please visit www.smartcardalliance.org

Trusted Computing Group (TCG)

The Trusted Computing Group (TCG) is an international industry standards group. The TCG develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and implementation by the industry. The TCG publicizes the specifications and uses membership implementations as examples of the use of TCG Technology. The TCG is organized into a work group model whereby experts from each technology category can work together to develop the specifications. This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.

For further information please visit: http://www.trustedcomputinggroup.org/

10. Information and Reference Sources

The current document contains appropriate references for definitions that have previously been covered by other bodies. Such references are also provided when further reading is available relevant to the respective term. The sources referred to are listed in this section with links to their respective websites. You can use the search engine on all of these sites to bring up any content pertaining to the search term.

Reference sources used in the document

- 3rd Generation Partnership Project (3GPP): http://www.3gpp.org/About-3GPP
- CDMA Development Group (CDG): http://www.cdg.org/
- EMVCo: http://www.emvco.com/
- European Central Bank (ECB): http://www.ecb.int/
- European Payments Council (EPC): http://www.europeanpaymentscouncil.eu/
- European Telecommunications Standards Institute (ETSI): http://www.etsi.org/
- Federal Financial Institutions Examination Council (FFIEC): http://www.ffiec.gov/
- GSM Association (GSMA): http://www.gsma.com/
- International Organisation for Standardisation (ISO): http://www.iso.org/iso/home/standards.htm
- Mobey Forum: http://www.MobeyForum.org/
- NFC Forum: http://www.nfc-forum.org/
- Smart Card Alliance: http://www.smartcardalliance.org/
- The World Bank: http://www.worldbank.org/
- World Wide Web Consortium (W3C): http://www.w3.org/

11. Further Sources of Information/Related Materials

Mobile Wallet Part 1: Definitions and Visions
For download at www.mobeyforum.org

Mobile Wallet Part 2: Control Points in Mobile Wallets
For download at Mobey Forum's Knowledge Centre www.mobeyforum.org

Mobile Wallet Part 3: The Hidden Controls: The unseen forces that will shape mobile wallet development.
For download at www.mobeyforum.org

Mobile Wallet Part 4: Structures and Approaches: the Changing Face of Mobile Wallet
For download at www.mobeyforum.org

The MPOS Breakthrough: How the Power of Mobile has Disrupted Payment
For download at www.mobeyforum.org

CI glossary for PCI DSS
By PCI Security Standards at www.pcisecuritystandards.org/documents/pci_glossary_v20.pdf