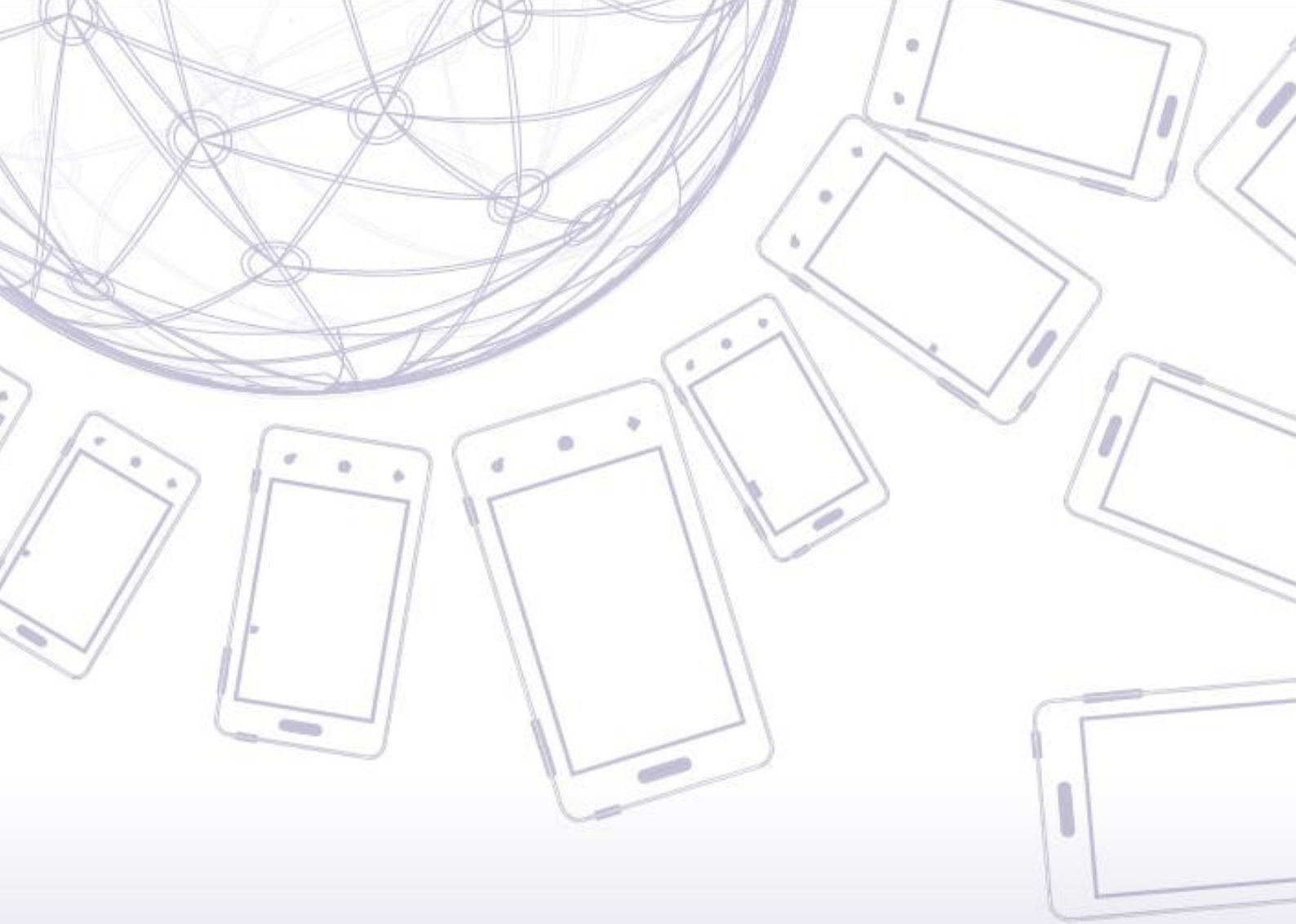


First Report of the Working Group on m-Commerce

m-POWERING DEVELOPMENT INITIATIVE

A BDT Initiative — Organized by ITU

m-Powering Development Initiative
Report of the Working Group on m-Commerce

Geneva, 12 May 2014

Executive Summary

Mobile solutions facilitate easy access to new markets and lead sustainable development with its potential to reach masses in the developing world. Mobile connectivity and increased use of mobile devices, therefore, provide tremendous opportunities for societies, businesses and governments to have wide range of services to be rendered practically at any time and any place.

During the uptake of mobile devices and mobile connectivity, businesses and governments recognised, to a great extent, the possibility of having commercial transactions by making use of mobile technologies. This led to the evolution of modern m-Commerce systems (including m-payment) which have become essential as no service could claim to be mobile without mobile payment arrangements. Due to its central role, m-Commerce is perceived as a tool to leverage all other mobile services.

m-Commerce systems have naturally emerged as a result of e-Commerce systems and during this process, they progressed from simple transfer of e-Commerce principles to mobile devices and to special applications, being stored and operating on mobile devices in protected environment, to provide strong multifactor authentication, data encryption and menu usability.

Consequently, mobile devices now tend to turn into “digital wallets” to store identification information on the wallet holder, on payment instruments accessible to the wallet holder and optional personal information items belonging to the holder.

The report focuses on the main characteristics of m-Commerce systems and it also provides an overview of various best practices.

1. Mobile-based services

Attractiveness of mobile devices for rendering remote services of m-Commerce, m-Health, m-Education, m-Government, etc. can be explained by many factors. First, mobile devices are the most widespread ICT devices. Due to success in the technology, modern mobile devices boast powerful core processors and provide high-speed communication channel, using 3G and 4G broadband networks. Thus, costs for devices and use of communication channels are quite affordable and have tendency to roll back. In 2014 the amount of mobile device users has nearly reached the amount of total population of the Earth.

Secondly, mobile devices are always “on the go” and are always “in use”, that allows to use services practically at any time, any place, even in moving transport. The great potential of mobile devices is proved by particular attention to them paid by numerous organizations, including the ITU, which has elaborated standards for the security of mobile financial transactions, while actively sharing experience in this area. During the research period of 2010-2014, the Study Group 2 of the ITU Telecommunication Development Sector (ITU-D) has developed the “Toolkit to create the ICT-based services using the mobile communications for e-government services” within the scope of Q17-3/2, to explain how to use these standards and to demonstrate how mobile-based systems are built in various countries.

In 2012, the BDT launched “m-Powering Development” initiative, which appears as an outstanding example of ITU activities, resulted in creation of several work groups, such as m-Commerce, m-Health, m-Sports and m-Education, aiming to summarize obtained experience in the use of mobile devices and to help developing countries to utilize such experience.

Mobile commerce systems (m-Commerce) have naturally emerged in the result of development of e-Commerce systems. During this evolution, they progressed from simple transfer of e-Commerce principles to mobile devices to special applications, being stored and operating on mobile devices in protected environment, to provide strong multifactor authentication, data encryption and menu usability.

Success in the technology, growing popularity of smartphones, and development in cryptography contribute to prospects of mobile devices for secure wireless payment, banking, and other remote transactions which require high protection level.

Mobile devices are offering large range of communication options, which can be used to provide remote services:

1. Voice-based services are available through voice communication with the operator of the call centre or IVR system. These services are convenient for old age people and visually impaired persons. They lack of high security level: information is openly transferred; authentication is carried out using the phone number and code words.
2. WEB-based services use the Internet services developed for desktop computers. Mostly, authentication is carried out using the password, sometimes with use of one-time passwords. Encryption is available with the use of SSL protocol, but these services are not so convenient to use on mobile devices due to their particularities (small screens, degraded keypad).
3. SMS or USSD-based services are specific features typical for mobile devices, allowing to order remote services by sending specially stipulated SMS or USSD. They lack of high security level and are not so user-friendly. Authentication is carried out via MSISDN, encryption is not

available. Due to insufficient security level they have limited list of services and restricted payment limits.

4. Services based on special applications in mobile devices or Secure Element are the most perspective and convenient method for users. Depending on implementation, they can have various security level up to the maximum (when using multifactor authentication, data encryption and operating within Trusted Execution Environment).

2. Classification of m-Commerce services

Mobile commerce consists of Mobile Financial Services and m-Marketing (see Figure 1 and Table 1). According to the Picture 1, MFS consists of m-Banking, m-Payment and m-money transfer. M-Marketing consists of mobile informing, mobile loyalty and mobile remote capture.

Figure 1: m-Commerce structure

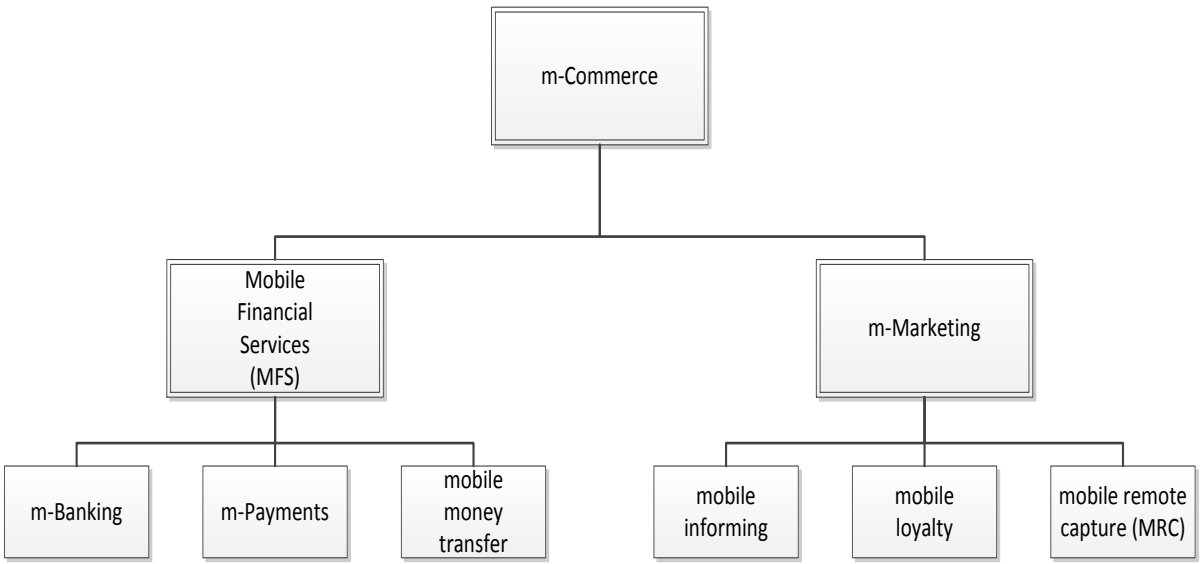


Table 1: Definitions

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.
m-Commerce	Mobile Commerce is the delivery of electronic commerce capabilities directly into the consumer´s mobile device, anywhere, anytime via cellular and wireless networks.
MFS	Mobile Financial Services is an umbrella term used to describe any financial service that is provided using a mobile device.
m-Marketing	Mobile **Marketing** is the marketing process, using mobile devices for communication with customers, for the purpose of selling products or services.
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.
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 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 informing	Mobile Informing is an information service, using mobile devices. The advantage of mobile informing is that information comes directly into the consumer´s device, anywhere, anytime via cellular networks. Examples of such services: bank informing, advertisement, etc.
mobile loyalty	Mobile Loyalty is a loyalty system, using mobile devices.
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 analyzed by 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.
MPS	Mobile Payment System

More terms and definitions used in mobile commerce defined in Definitions Whitepaper (http://www.mobeyforum.org/whitepaper/mobile-financial-terms-explained-2/), issued by Global Mobile Commerce Forum. This document can be found in the Annex 1 «Mobey Forum Definitions Whitepaper».

3. m-Commerce key drivers and key issues:

Table 2: Summary of key drivers and key issues

Key drivers	**m-Commerce**
	High penetration of mobile devices
	Always "on-line"
	Fast growing capabilities of mobile devices
	Trust
	Easy to use: comfort
	Cost savings
	Previous experience of Internet shopping
	Business opportunities
Key issues	
	Security
	Convenience and availability
	Regulation/Legislation
	International Standards
	Affordability

3.1. Key drivers

While talking about *"high penetration of mobile devices"* and being *"always on-line"* as key drivers, it is essential to distinguish between mobile phones and those mobile devices, like tablets, that need not always be connected to a network. Mobile phones need to be continuously connected to the mobile network. Other mobile devices such as tablets may only be connected sometimes to the Internet. For a developing country, the mobile phone may be of greater relevance due to their ubiquitous presence and continuous connectivity to the mobile network. Devices such as tablets may be less significant due to low levels of penetration of Internet and broadband, at present. Hence, drawing a distinction between mobile phones and other mobile devices and between mobile phone networks and the Internet will help to focus attention on the relevant key drivers in different countries.

"Fast growing capabilities" of mobile phones, with more varied modes of making transactions, applications or programs in local languages that could remove the language barrier to entry and use of mobiles for banking etc. are key drivers to growth of m-banking and m-commerce.

"Trust", "ease of use" and *"cost-effectiveness"* are crucial drivers for the establishment and growth of m-commerce services. To engender trust in m-banking, it is important to not only ensure the security of money in the mobile or bank account but also the security of underlying mobile transactions. This can be a key driver for increase in the banked population in rural and remote regions of developing countries where the use of traditional forms of banking is seen as a complex and cumbersome process, further restricted by the limitations of transportation and social structure. A person could be giving up an entire day's wages just in order to make a trip to the bank to undertake a financial transaction.

Use of ATMs and carrying cash from one place to the other is also extremely unsafe. M-banking as a safer alternative would bring this large hitherto-unbanked population into the ambit of banking services. As the target population is largely not literate or tech-savvy, it is essential to make the transaction process simple and easy to comprehend, with the language of communication not acting as a barrier. A well-established customer complaints redressal system in case of failed transactions would further establish trust in the system. Mobile banking would also be so much cheaper for the banking organization which would otherwise have had to set up bricks and mortar outlets to reach such populations.

"Previous experience of Internet shopping" may aid in building familiarity with the system among customers for m-commerce. However, Internet penetration in developing countries is very limited, especially among the poor in remote regions; therefore such previous experience is likely to be limited. This would not stand in the way of growth of services such as m-banking using simple interfaces over mobile phone devices. Experience of Internet shopping may be useful for system enablers and system providers.

As regards *"business opportunities*", establishment of new business entities like aggregation platform providers that provide a common platform to connect several banks and telecom service providers (TSPs) has eased the transaction process and proved to be a key driver for growth of m-banking. Such platforms, by improving efficiency and merchant-buyer interactions also encourage the entry of more merchants into doing business, thus further facilitating opportunities for business.

3.2. Key issues

"Security" is most essential as it engenders trust and faith. The regulations in this area should also include protection of privacy of transaction data. *"Convenience"* is tied to ease of use and device capabilities; *"availability"* is tied to the spread of devices amongst traders, and enhanced by network effects. Though *"regulation"* by telecom and banking regulators is vital, greater clarity will be required on *"legislation"* as a key issue in the present context i.e. what exactly are the areas in which legislation will be required? *"International standards"* are good for setting interoperable platforms across countries and also to set technological standards for various modes of transactions, for example, IVRS, SMS or USSD based mobile transactions. The role of international standards is very important for security aspects.

"Affordability" is another key issue which needs to be considered – should the customer or the bank pay the telcos for the m-banking services rendered? The bank, though saving costs by increasing the customer base without incurring the usual costs of opening a branch, ATMs etc., is not able to make profits out of the zero balance accounts maintained by the targeted population that is largely poor.

4. Main stakeholders

Table 3: Main stakeholders

Main stakeholders	**m-Commerce**
Customers	+++
Professionals in technology and services	+++
Gov. /Regulatory bodies	++
Banks	+++
Telco Operators	+++
Services & App providers	+++
IT Technology Vendors	++
Content providers	+
International Organizations	++
Funding/Sponsors	+

The average customer, who has no alternate means of access to banking and financial services, in our view, is the central stakeholder and the m-banking framework must essentially target such people.

Inclusion of banks as stakeholders is important, as they perform key functions in m-banking in a bank-led framework as well as a telco-led framework, as transactions from the bank account will require the connectivity between the telco and the bank, possibly through a banking platform. It is also most essential to include the relationship between the banking and telecom regulators and their responsibilities in the m-banking framework. The eco-system around the m-commerce transaction needs a reliable communication carriage system and a stable payment settlement mechanism that would be governed by regulations of the telecom and the banking sectors respectively.

5. Requirements for m-Payment systems

To date, there are many payment systems are called mobile payment systems (MPS). Below is described a certain perspective model of the current MPS.

Two operation types should be available in MPS:

- Operations initiated by Clients (including P2P transactions)
- Operations initiated by Merchants

For implementation of the listed above payment types the unique identifier (ID) should be assigned to each user of MPS. User's mobile phone number MSISDN (International Standard E.164 ITU-T) appears as the most convenient User ID, as users normally remember their phone numbers and therefore, they will

not have to memorize one more ID. Besides, ID may be digitally entered into those devices, which are limited to having only a number pad, for example, ATMs. At the same time, users will be allowed to bind their digital ID to any unique pseudonym defined by the user. In certain cases, pseudonyms will allow users not to disclose their telephone number when carrying out transactions.

The user can have several means of payment (numerous bank accounts, payment cards, mobile network operator accounts, operators of e-money payment systems, etc.). Thus, each means of payment is provided an alias during its registration. The user, after having received a payment request from the seller, will have an opportunity to select any of them.

As an example: User decides to make payment in the restaurant and tells his pseudonym or telephone number to the garcon, who initiates the payment request on the restaurant payment system. This request is forwarded by the system to the payer according to his ID, and the payer, if agreed to pay on demand, selects available means of payment from the ones previously registered in the payment system and returns the response to request, providing alias for selected means of payment. The payment system uses the alias to find out the holder of means of payment and appropriate account.

The following means of payment may be used as sources for Mobile Payment Systems:

- Bank accounts
- Bank cards issued by local or global payment systems, including virtual cards
- MNO subscriber's personal accounts
- Other accounts with cash deposit and withdrawal
- E-money

As for the state financial system, it is mandatory that the share of cashless payments shall be maximal. As cashless payments are carried out by banks, these payments cannot be anonymous. That allows the state to control income and expenses of citizens and to counteract illegal business. Besides, non-cash money are not kept in a piggy bank, but actively used by financial system, what increase the velocity of money, i.e. the rate at which stock of money is passed round the economy as people transact. This also appears as a positive factor for the state. In some jurisdictions, the Central Bank may be reluctant to permit non-banking entities to function as banks i.e. they may favour a bank-led means of payment including bank accounts and payment cards. However, it is necessary to consider that use of cards issued by international payment systems draw additional contributions to these systems, and also allows them to manipulate payment services.

Therefore, all non-bank means of payment are unwanted for the state, but from users point of view they may be attractive due to their easy-to-subscribe feature, and in certain cases due to anonymity of payments.

Inconsistency of these two tendencies can be resolved by limiting of non-bank payment amounts and by the following measures:

- Licensing and registration processes
- Customer identification
- Record keeping
- Internal controls and monitoring
- Guidelines
- Reporting obligations

- Supervision and oversight
- Preventive framework for cross-border transactions
- Staff training

6. Advanced solutions of m-Payment system

As it was mentioned before, the most convenient system for users is the one with applications pre-loaded onto mobile phones. Applications provide multifactor user authentication, encryption and decryption of transferable data; they also offer the user menu facilitating transactions. Entire application or part of the application with sensitive data shall be stored in the Secure Element, which can be a SIM/UICC card, built-in storage, or special tamper-proof SD card. Usage of SIM/UICC cards as a Secure Element looks very attractive, but makes the provider of m-Commerce services dependent from the mobile network operator which owns these cards. As it was noted by GSMA, which has been involved in discussions with the European Commission since 2001 on various approaches on how mobile operators are entering the domain of financial services:

- Mobile operator as a provider of telecommunications services only
- Mobile operator as a provider of financial services

Some opportunities presented by industry convergence from both the mobile operator and the consumer perspectives are listed below:

- **Complementary capabilities** - mobile operators and financial institutions have different strengths and histories in these areas and significant work is necessary to deliver a good mix of capabilities combining financial services offered by financial institutions and broad reach of consumers offered by mobile networks.
- **Ease of use** – as financial services and telecommunication services converge, it becomes possible for the mobile handset to perform a new array of digital services. The ease of use offered to both mobile subscribers and users of financial services is driving both industries towards a more inter-connected world.
- **Transparency and traceability** – all digital activities can be traced and the same is true of digital financial services. Using a mobile handset to pay for goods can allow both the payer and the payee to have access to transactions logs adding more transparency and traceability to the activity compared to cash transactions.
- **Servicing un-served markets** - many mobile money operators will look to capitalise on the ubiquity of mobile networks where financial services lack reach, as in the case in many developing nations. The value to the mobile subscriber is financial inclusion. For the mobile operator and a range of other service delivery agents, new revenue opportunities arise. The nation as a whole can benefit from the general uplift in commerce and the alleviation of poverty.
- **Servicing under-served markets** – financial institutions suffer additional costs on maintaining both cash-based and card-based payment systems. Furthermore opportunity cost results when traditional banks do not extend their services to low-value customers. Mobile money operators take advantage of the ubiquity of mobile handsets and networks to deliver low cost financial services to capture the high volume, low value transactions in a cost effective manner.
  In line with the context described above, the GSMA is committed to supporting the development of interoperable services in this area, in order to lower costs, increase choice and help the market grow in a sustainable way.

However, in some countries financial services are only authorized to be offered by banks. It does not allow mobile operators to appear as mobile payment operators. According to obtained experience, mobile network operators reluctantly cooperate with banks and that slows down the development process. So, tamper-proof microSD cards appear as an alternative for SIM/UICC cards which allows banks to be independent from mobile operators as mobile payment service providers.

It is well-known that reliability of authentication is reached by a multifactor authentication, which is the combination of three factors:

- Something you have (mobile device with the special application)
- Something you know (password or PIN code)
- Something you are (biometric)

Normally, two-factor authentication is used in regards to the first two factors. PIN or password known only to the user is used in the mobile device to protect against unauthorized application launch by the intruder. However, the technology development is very rapid in our times, and new solutions and opportunities pop up constantly.

The most recent and interesting developments -from financial services perspective- seem to be happening in Biometrics, with some of the most prominent companies taking baby steps in implementing biometric solutions for that (PayPal, Samsung, Apple TouchID. etc.). There is a constant demand to know and learn more, and be up to date on what are the most promising technologies available and by whom. Lately, due to efforts of Natural Security Alliance association, the standard of biometric authentication with the use of fingerprints is promoted. Biometric authentication can replace entering PIN. Otherwise, two-factor authentication may become three-factor authentication with the use of biometric authentication.

For higher security mobile devices shall be able to provide so-called Trusted Execution Environment (TEE), which protects from data interception transferred between units within the mobile device, for example, between the keypad or the display and the Secure Element where the application is stored. An application should contain minimum of sensitive information and store only the data required for user authentication and encryption keys. All remaining information, including credit card data or accounts data should be securely stored within the server by the payment system operator. Such allocation not only provides higher security level, but also facilitates creation of new services and modification of existing ones with the minimum interference in the mobile device.

The following factors define successful practical implementation of the system:

1. Costs of system creation and maintenance
2. Financial losses due to fraud
3. Usability for customers

Obviously, these factors contradict with each other. Usually, higher security level requires less convenience for users and higher costs of works on creation and maintenance of the system and thus, the clients shall pay more for the use of the system that can appear as turn-off factors. As it was mentioned above, risks may be decreased by reducing system's functionality, however, that will lower its popularity. According to users' preferences, the system should be simple, convenient and elegant. This can be reached by special applications pre-loaded onto mobile phones.

Importance of some parameters is differently perceived in different regions. Such parameters are functionality and security. So, m-Pesa system, despite lower functionality and insufficient security, has gained huge popularity among several African and Asian countries. However, it is difficult to imagine that such a system will become popular in Europe or North America, where user requirements to security and protection are essentially higher. The success of m-Pesa system in the mentioned-above regions is due to its accessibility, low prices and poor development of banking sector at a high demand of financial services traditionally provided by banks. Initiatives in utilizing mobile technologies to facilitate payments have successfully brought financial services to the doorsteps of billions of unbanked poor people. One can conclude, that the most attractive factor for developing countries with under-banked population is service availability, including cost of service use, while in developed countries the great value is given to security and service functionality. This can be a bright illustration of the fact that currently developed and developing countries have different requirements for m-Commerce Systems. Nevertheless, no doubts that the future belongs to multifunctional and secure systems, when such systems will become available and reasonably priced.

7. Security of mobile payment systems

Prior to the era of smart phones, management of mobile applications by operators on mobile phones was relatively easy. Basically, operators used to control which application can be downloaded onto device and their security characteristics. Management of mobile applications becomes more complicated with the advent of smart phones and ability to freely download third party applications. Nowadays, it is almost impossible to be completely certain that every application that is executing on a mobile device originated from a trusted source.

As a result, mobile users are subject to additional threats such as identity theft, phishing, and loss of personal data. So, one of the most important requirement for payment systems, as well as e-government and e-health systems, including their mobile variations, is security, which is provided by meeting recommendations of the ITU Telecommunication Standardization Sector, which issued a manual entitled "Security in telecommunications and information technologies". This manual provides an overview of existing ITU-T Standards and their practical application in secure telecommunications. ITU-T Standards are required to follow, they stay as recommendations, but compliance with recommendations is essential to ensure compatibility and consistency of telecommunication systems of different countries. Some of these Recommendations are related to any kind of telecommunication networks, others are made especially for mobile networks and few of them are elaborated for mobile payment systems. Nevertheless, all of them are mandatory to comply with.

Since mobile commerce systems involve many players, security considerations can be divided in multiple categories that include:

1. End-point Security
2. Mobile Application Security
3. Mobile Network Security
4. Identification of the requesting party that includes proper identification of the individual that is requesting the financial transaction.

The term "security" is used in the sense of minimizing vulnerabilities of assets and resources. An asset is anything of value. Vulnerability is any weakness that could be exploited to violate a system or information it contains. A threat is a potential violation of security. The ITU-T Recommendation X.805

"Security Architecture for Systems Providing End-to-End Communications" (Figure 2) defines set of eight so-called "Security dimensions" – set of means that protect against all major security threats, described in the ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications".

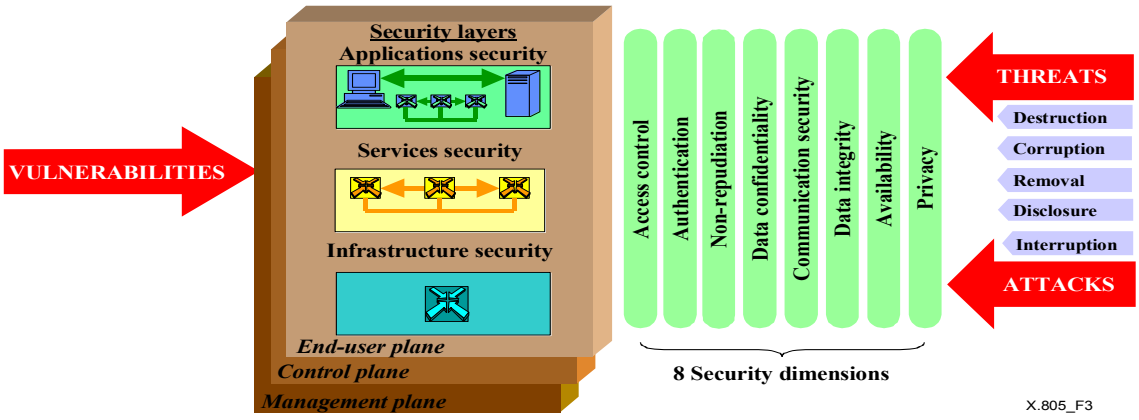
These security treats are:

- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;
- information disclosure;
- service interruption.

Security dimensions are not limited to the network, but extend to applications and end user information as well. In addition, security dimensions apply to service providers or enterprises offering security services to their customers. These security dimensions are:

1) Access control;
2) Authentication;
3) Non-repudiation;
4) Data confidentiality;
5) Communication security;
6) Data integrity;
7) Availability;
8) Privacy.

Figure 2: Recommendation X.805 – Security architecture for end-to-end network security

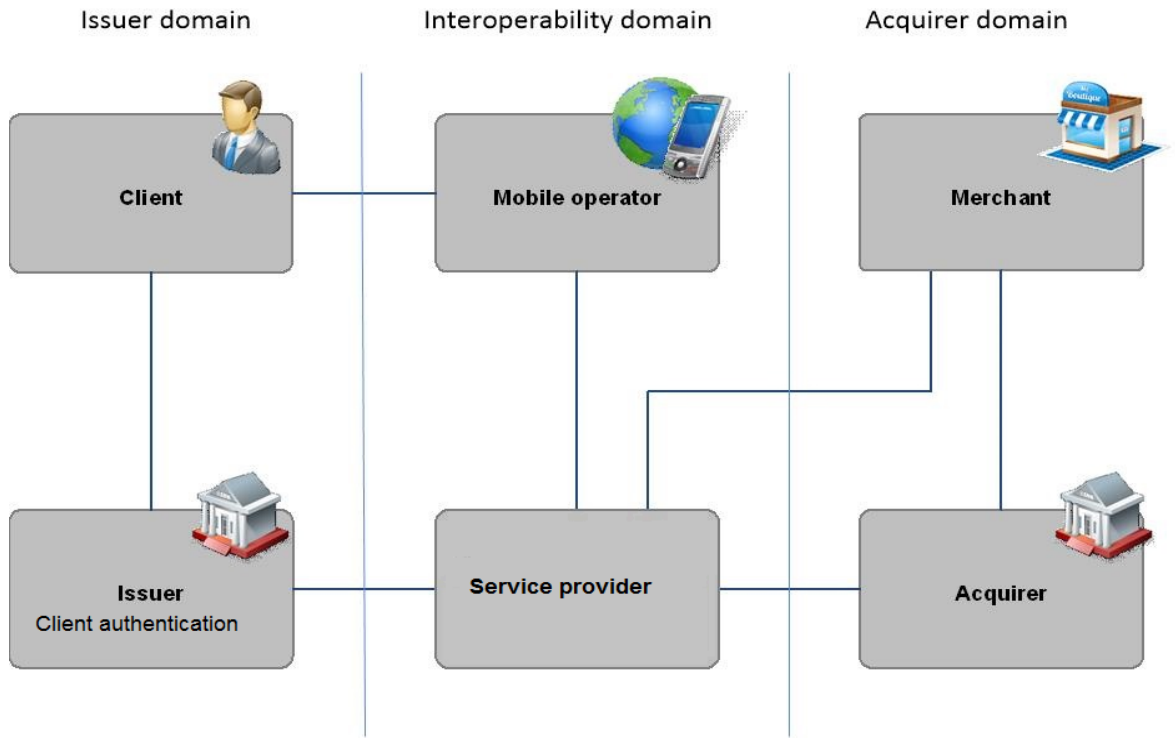


The ITU-T Recommendation X.1122 applies when using asymmetric cryptography, and provides guidelines for creation of secure mobile systems based on Public Key Infrastructure (PKI). This standard describes generation of public and private keys, certificate applications, as well as issuance, activation, use, revocation and renewal of the certificate.

The ITU-T Recommendations Y.2740 and Y.2741 describe security requirements and architecture of secured mobile financial transactions. These recommendations, though made for mobile remote financial transactions in NGN, are fully applicable to ensure security for m-Payment systems in 2G, 3G

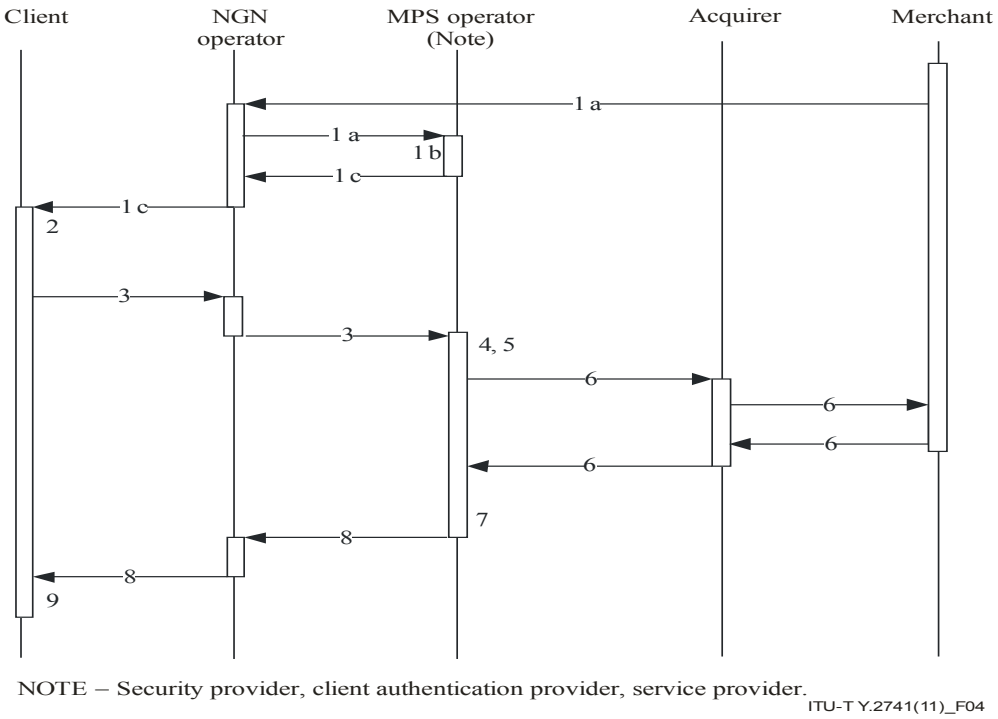
and 4G mobile networks. The Recommendation Y.2741 “Architecture of secure mobile financial transactions in next generation networks” describes the system architecture and possible interaction scenarios. This 3-domain architecture of m-Commerce system, compliant to “3-D Secure” protocol with multifactor authentication is provided below (Figure 3).

Figure 3: 3-D architecture of m-Commerce system



In this architecture the authorization of financial transaction is carried out by the Issuer as a result of final authentication made by issuer’s authentication system. Preliminary authentication, as well as provision of security for transmission and storage of sensitive data should be performed by the Service provider. In some cases roles can be combined, for example: Issuer and Service provider (bank-owned system) or Issuer and Acquirer (P2P money transfer within one bank), or even all roles, except Client (mobile operator top-up system). Scenario for Merchant - initiated payment is shown on Figure 4.

Figure 4: Scenario for Merchant initiated payment (ITU-T Recommendation Y.2741)



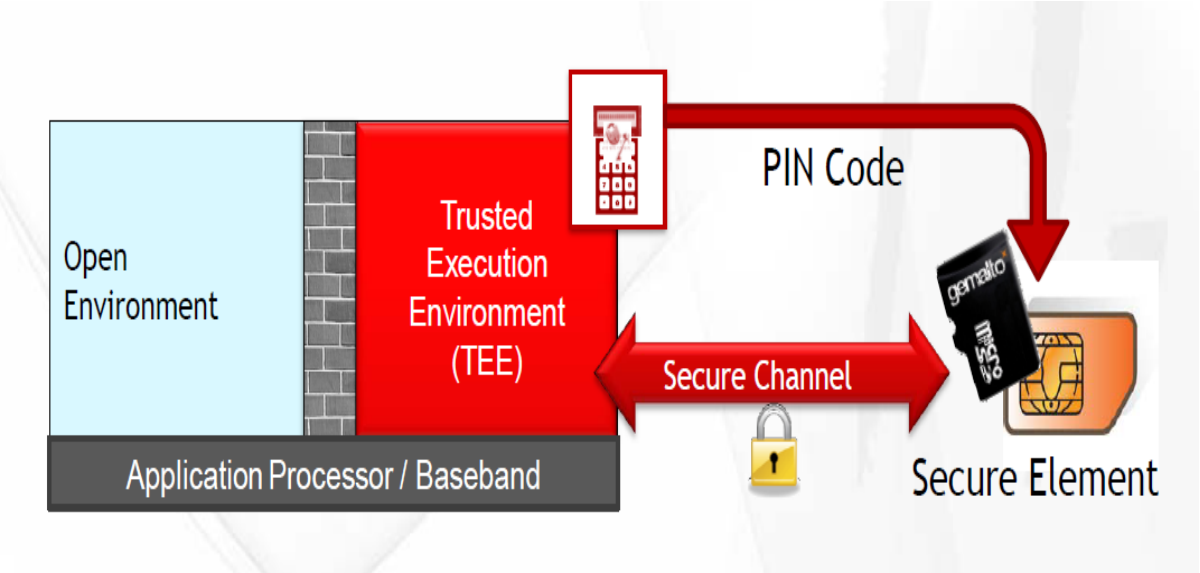
The Recommendation Y.2740 “Security requirements for mobile financial transactions in Next Generation Networks” defines four security levels of mobile financial transactions systems depending on implementation of security dimensions (see Table 4). Thus, the fourth (the highest) security level must have the strongest implementations of security dimensions.

It is necessary to say that for the Security Level 4 obligatorily to have a mobile device with Trusted Execution Environment. TEE is a secure area that resides in the application processor of an electronic device (see Figure 5). To help visualize, think of a TEE as somewhat like a bank vault. A strong door protects the vault itself (hardware isolation) and within the vault, safety deposit boxes with individual locks and keys (software and cryptographic isolation) provide further protection.

Separated by hardware from the main operating system, a TEE ensures the secure storage and processing of sensitive data and trusted applications. It protects the integrity and confidentiality of key resources, such as the user interface and service provider assets. A TEE manages and executes trusted applications built in by device makers as well as trusted applications installed as people demand them. Trusted applications running in a TEE have access to the full power of a device's main processor and memory, while hardware isolation protects these from user installed apps running in a main operating system. Software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other.

Device and chip makers use TEEs to build platforms that have trust built in from the start, while service and content providers rely on integral trust to start launching innovative services and new business opportunities.

Figure 5: User verification in Trusted Execution Environment



The era of mobile devices with the TEE is just started, but this technology will protect in nearest future the Achilles heel of the nowadays mobile payment systems.

Table 4: Four Security Levels of MPS (ITU-T Recommendation Y.2740)

Security Dimension	Security Level			
	Level 1	Level 2	Level 3	Level 4
Access Control	The access to every system component shall be granted only as provided by the System personnel or end-user access level.			
Authentication	Authentication in the System is ensured by mobile network data transfer environment	Single-factor authentication at the System services usage	Multi-factor authentication at the System services usage	In-person connection to services where personal data with obligatory identification is used. Multi-factor authentication at the System services usage. Obligatory usage of Hardware Cryptographic Module.
Non-repudiation	The impossibility of a transaction initiator or participant to deny his or her actions upon their completion is ensured by legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users.			

<table>
<tr><td>Data confidentiality</td><td rowspan="2">Data confidentiality during the data transfer, is ensured by the data transfer environment (communications security), and by the mechanism of data storage together with the means of system access control – at data storage and processing.</td><td rowspan="3">Data confidentiality during the data transfer is ensured by additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking together with well-defined distribution of access in concordance with privileges and permissions.</td><td rowspan="3">The implementation of the Level 3 requirements with the obligatory usage of hardware cryptographic and data security facilities on the Client's side (Hardware Cryptographic module).</td></tr>
<tr><td>Data integrity</td></tr>
<tr><td>Privacy</td><td>Privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities.
The System components must not have latent possibilities of unauthorized data acquisition and transfer.</td></tr>
<tr><td>Communication</td><td colspan="3">The delivery of a message to the addressee is ensured as well as the security against unauthorized disclosure at time of transfer over the communications channels. It is ensured by the NGN communications providers.</td></tr>
<tr><td>Availability</td><td colspan="3">It ensures that there is no denial of authorized access to the System data and services. Availability is assured by the NGN communications providers as well as the service providers</td></tr>
</table>

Requirements for some security dimensions are unified for all security levels. Parties using MPS should be aware of the System security level and the System's risks. The acceptable security level for a certain risk of any System component is determined by the party taking this risk. As risk rate is the function of the security level and the amount of potential losses in the event of security violation, parties can additionally mitigate the risks of using MPS by operational measures which may include limiting the frequency or monetary value of individual transactions, the availability of the service to users with high loyalty level, etc. As an example, there are mobile top-up services exist for mobile operators without any security, but with no risk, because they only allow users to top-up their own accounts on a limited sums by using SMS.

Besides ITU standards on security, the WG recommend also to study the European Central Bank's "Recommendations for the Security of Mobile Payments" (which is currently draft document issued for public consultation).

8. m-Commerce initiatives in different countries

In India

In India, telcos are allowed to provide only closed and semi-closed wallets to their customers i.e. a telco customer who subscribes to an m-wallet service has access to only a limited range of payment options. Bank-led m-banking initiatives have however been encouraged by the Reserve Bank of India (RBI) through Business Correspondents (BC), who are agents of the bank facilitating the unbanked population in remote areas in opening bank accounts. Though cash deposit and withdrawal have to be performed with the BC personally, other types of transactions like transfers and payments can be carried out by the account holder using the mobile phone. As m-banking transactions involve multiple banking and telecom interfaces, a framework involving aggregation platform providers has been established to ease the transaction process and enhance the efficiency of the m-banking system. The RBI has also appointed a Technical Committee on Mobile Banking to examine various options for providing m-banking services, including the feasibility of using encrypted SMS based funds transfer.

The objectives of the m-banking project in India are:

- Low-cost/ free of cost access to financial services (anytime access and low transaction costs)
- Quick and easy operability (transaction in most basic of sense, minimum paper work)
- Security and safety of public money (trust and reliability)
- Less obtrusive operational requirements (minimum balance requirement, daily transaction limit, minimum activity requirement etc.)
- Possibility of making frequent deposits and remittances

In India, Unstructured Supplementary Services Data (USSD) has been identified as an appropriate communication channel for m-banking services for financial inclusion, as it is available in almost all handsets and requires no additional application or accessories, which makes it attractive for use by someone with a basic mobile phone model. Hence, it is convenient, easily available, accessible and inexpensive.

The Telecom Regulatory Authority of India (TRAI) has taken steps to regulate tariffs for use of communication channels of telcos for m-banking transactions as well as the quality of services. TRAI has prescribed an affordable ceiling tariff of Rs 1.501 per outgoing session for the customer for the use of USSD communication channels and has established a framework to facilitate banks and platform service providers to interface with telcos for use of not only USSD, but also SMS and IVR (Interactive Voice Response) channels to provide m-banking services.

From an implementation point of view, it is useful to set up a hierarchy of the various banking and financial services that can be used on a mobile phone as follows:

Rudimentary banking services – deposit, information and transfer facilities

(ii) Advanced banking services – payments between accounts like bills including utilities, payments for credit cards, merchant payment settlements.
(iii) Payments for day-to-day transactions e.g. payments at grocery stores, MPoS solutions
(iv) Large transactions that are presently carried out on the Internet.

In Russia

Various mobile payment systems have become very popular in Russian Federation. Some of them, while having minimum functionality limited to top-up the balance of previously registered mobile phone, do not require security and, respectively, do not provide it, the others (for example, mobile payment systems "Easy payment" and "MasterCard Mobile"), have wide functionality and meet high security level requirements, set forward by ITU standards to secure systems. Thus, and this is very important, security means do not invoke any additional inconveniences for users. All the diversity of means presented by modern mobile communication standards is used as transport environment. SMS and USSD have become quite wide spread, however, due to wide circulation of smartphones and development of standards for mobile telecommunication systems, increased the use of GPRS, UMTS and LTE.

It is interesting to note, that in the market under equal conditions are present both applications with “sensitive information” stored on tamper resistance devices, and applications with the data stored in the phone’s memory. Nevertheless, the latter have become more popular, yet they are potentially less secure. Obviously, the consumer benefit of the latter is that he does not need to change his SIM/UICC card. Yet, risk of reading the confidential data from phone’s memory is a shortcoming. With respect thereto, it is interesting to compare these two types of applications from the point of security.

According to statistics, fraud usually takes place not when applications on stolen phones are hacked, but either because of the “human factor”, or virus programs penetrated into clients’ phones. And this is the least protected system elements, that requires further increase of security of mobile applications only in case of very high risks of being hacked, for example, for the official digital signature recognized by state entities. Unlike it, risks of payment systems can be limited by the maximum amount of financial transaction per transaction and/or a time period. Therefore, the most important role in secure usage of devices working in open networks consists of training clients to use these devices, and to use anti-virus programs. Thus, certainly, the service provider should take all measures to protect confidential information, defined by ISO 27001 and other similar standards. In particular, it is necessary to minimize amount of employees operating the system, who have access to “sensitive data”, to assign different access levels to the system, and to provide mandatory authentication and login registration.

9. Recommendations

- Since mobile phones have achieved full market penetration and high service levels, they are the ideal payment terminals and secure communication instruments.
- It is important to provide easy-to-use mobile phone interfaces with consistent user experience across all supported mobile phone implementations; even if the most advanced smart phones boast “great” color displays and touch-based interfaces. The user experience remains strongly challenged by necessarily small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text. Thus, it looks like good idea to make unified e-Commerce systems both with the use of laptops and mobile devices and to give a user to choose device to use dependent on the situation.
- Mobile device is a “digital wallet”, to store identification information on the wallet holder, on payment instruments accessible to the wallet holder and optional personal information items belonging to the holder (e.g., pictures, documents, etc.). This may include information related to ID cards, digital signatures and certificates, logon information, billing and delivery addresses as well as

payment instrument related information. Furthermore, it may also include other applications such as loyalty, transport or ticketing.

- It is advised that Customers should not be bound to a specific MNO or Bank, and should retain their current ability to choose service providers.
- Parties of electronic dialog should be authorised with the use of at least two-factor authentication, and data transfer should be executed in secure mode using cryptography means.
- It is advised to use Security Level 4 or 3 according to Y.2740 ITU-T Recommendation.
- Customers should be aware of the Security Level of the System, which should be stipulated in the participants' agreement. User authentication may be performed by the Unified centre of authentication.
- To ensure the security and to be user-friendly, the mobile device must have a special Mobile Application, which provides authentication and encryption.
- The most realistic vision is one of a market where multiple Mobile Applications co-exist, combining services on a single mobile device.
- The registration and provisioning of a Mobile Application needs to be executed in secure environment. Access to a Mobile Application would be easier for customers, if they could use existing trusted relationship between them and their service providers.
- To reach the highest security level, Mobile Application should be located on the hardware Security Element.
- The choice of Security Element has a major impact on the service model and roles of various stakeholders. There are three types of SEs used until now: UICC, embedded SE and removable SE, such as micro SD card.
- Service Enabler provides the technology support and integration of various access means, interoperability with service providers and authentication centre.
- It is recommended to use Mobile Applications with several independent blocks with different sets of keys.
- The Client may have multiple customer mobile identities – mIDs, bounded to the Client's MSISDN. Unified rules to issue mIDs, registered within the System Central Directory, should be introduced to ensure proper routing of messages to Clients.
- All identification and authentication centres must comply with the same allocation rules and regulations for mobile identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.
- Mobile systems should, as much as possible, use technologies and infrastructure which have been already widely deployed.

10. Conclusion

The most advanced today's systems which are based on mobile devices offer the whole range of services which is continuously extended. So, beside mobile payments and mobile banking services, wide application was received by services based on geolocation. Besides, it is stated at White Paper Mobile Payments 18, issued by European Payments Council in 2012, the mobile terminal should represent a "digital wallet" which will provide authentication and digital signature to replace multiple passwords, IDs and loyalty cards of merchants (Figure 6).

Figure 6: The digital wallet is replacing the leather one

As a normal wallet, the "digital" wallet, in effect, contains identification data of the owner, data on means of payment available to the owner, and in certain cases - personal data of the owner (images, documents, etc.). It may include ID information, digital signatures and certificates, login information, addresses for drawing of scores and transmission, and so on. Besides, it can also include other applications, for example bonus points, tickets or travel documents.

After having passed authentication in Authentication Centre, one may enter personal merchant accounts or social networks, such as Facebook, Linkedin, etc., which is very convenient and relieves from the need to remember or to store securely numerous passwords of multiple accounts. In the short term, one can expect active use of mobile devices as terminals for e-government and healthcare. The m-Powering Development Initiative, launched at Telecom-2012 by the ITU-D, is to prove this statement.

Annex A

Membership of Working Group on m-Commerce

Members drawn from m-Powering Development Advisory Board:

Mr. Evgeny Bondarenko (Chair)

Mr. Rahul Khullar

Ms. Anne Bouverot

Mr. Yury Grin

Mr. Sipho Maseko

Colleagues supporting members of the Advisory Board:

Mr. Andreas Schauer

Ms. Marina Solin

Ms. Belinda Exelby

Annex B

Mobey Forum Definitions Whitepaper

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.
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.
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 realized. SMS messages are always sent through the SMSC (the Short Message Service Center) of the subscriber'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.
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.
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. Source: 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 (i.e. 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.
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 frequencies 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 personalization 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 initial point where data is entered 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, personalized 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, GlobalPlatform, 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: GlobalPlatform.

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 personalization 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.
Mobile Money	Mobile Money is a very general term meaning any financial action made with a mobile device.
Mobile remote payment	A payment initiated 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 analyzed by 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.
MPS	Mobile Payment System