M-Payments Issues and Concepts

Cristian TOMA
Department of Economic Informatics and Cybernetics
Academy of Economic Studies Bucharest
cristianvtoma@gmail.com, cristian.toma@ie.ase.ro

The paper has four sections. First section has an intro for the mobile payments requirements for a reliable service. Second section shows types and models of mobile payment service but not taking into account the service patterns and the electronic money systems. In section three as a case study is shown an author solution may be improved taking into account the security and ergonomic issues presented in the first two sections. The last section presents a summary of technologies available for improvement of the mobile payment services.
Keywords: *2D Barcode, DOV – Data over Voice, NFC – Near Field Communication, Mobile Micropayments, Ticketing System*

1 M-Payments Introduction

The paper Mobile payment (M-Payment) is a field with an economical grows supported by the decreasing costs of GSM communications, devices and applications. An important factor for m-payments grow is the end-user awareness and the products and services compliancy to fast and simple payments methods.

The products and goods that can be achieved with the m-payments methods could be:

- Electronic content: Applications, e-Books, games, VOD – Video on Demand, music, ringtones, wallpapers, etc.
- Hard goods: Concerts tickets, Books, journals, magazines, etc.
- Services access: transportation fare – bus, subway or train, parking meters, cinema access and other services.

According with [1], a mobile payment service should meet the following conditions in order to be trustworthy within the markets:

- Simplicity & Usability: The m-payment application should have an ergonomic GUI – Graphical User Interface with small learning curve to the customer. The application's personalization is a criterion for the end-user satisfaction.
- Universality: M-payments service should be possible for low value micro-payments and high value macro-payments and it should include domestic, regional and global environments.
- Interoperability: The m-payments service should be able to interact with other systems and it should be based on open standards and technologies.
- Security, Privacy & Trust:
  - As an objective the mobile payments have to be as anonymous as cash transactions.
  - If the mobile payments system is not anonymous, then a customer must be able to understand how his or her private information is protected and the client must be sure that is hard or impossible to expose this information (e.g. credit or debit card) to other entity from the payment system (other than the client, merchant or bank).
  - Also, when mobile payments transactions are recorded, the customer privacy should not be openly available for the public access – the credit histories and spending patterns of the customer.
  - The system should be "bullet-proof", resistant to inside or outside attacks. A solution is to use public key infrastructure security, specialized crypto-chips (embedded or external to the mobile device), biometrics and passwords integrated into the mobile payment solution architectures.
- Cost: From macro and micro systems point of view the costs of the usability and deployment for the m-payments systems should be lower than the existing

payment mechanisms.
- Speed: The speed of the mobile payments execution should be acceptable to customers and merchants.
- Cross border payments: The m-payment application and transactions should be available globally, in order to be widely accepted – regional or world-wide.

Also the mobile payments methods are dynamically modified by the technological evolutions and by the end-user experiences. In the following sections, there are presented various types of mobile payments methods and systems.

2 Types and Models of Mobile Payments

One of the main problems is which entity is going to provide the support for the financial infrastructure: the bank, the mobile operator, other private or public company, or a consortium. According to [2], there are three different models available for m-payment solutions on the basis of payment:
- Bank account based
- Credit card based
- Telecommunication Company billing based.

Mainly, the mobile payment service is provided taking into account one of the following models [3]:
- Operator-Centric Model: The mobile payment service is deployed independently by a MNO – mobile network operator. An independent mobile wallet with electronic cash or money (stored in the SIM, internal/external crypto-chip to the mobile device or software application) may be provided by the mobile operator. The charging of the electronic wallet may be done through the user mobile account (telephony company bill) and the money withdraw may be done using specialized offices with mobile operator agreement. Mobile network operator should be interoperable with the bank network in order to provide advanced mobile payment service in banked and under banked environment.
- Bank-Centric Model: The mobile applications or devices are provided by a bank to the customers for the mobile payment transaction achievement and the bank provides to the merchants the compliant point-of-sale (POS). Mobile network operators are used as simple carriers or device providers.
- Collaboration Model: The banks, mobile operators and a trusted third party are collaborating for providing the mobile payment service, including the issuing of co-branded devices that ensures the customer loyalty.
- Peer-to-Peer Model: A private/public institution or company, independently from financial institutions and mobile network operators, is the mobile payment service provider.

The mobile payments service may or may NOT include electronic money (also known as e-currency, e-money, electronic cash, digital money, digital cash, cyber currency) exchange.

Examples of electronic money are [5]: EFT – Electronic Funds Transfer, direct deposit, digital gold currency and virtual currency united under the term of "financial cryptography". There are three types of electronic money systems:
- Centralized Systems – sell their electronic money directly to the customer (e.g. PayPal, WebMoney, netCash.is, Payoneer, cashU, Hub Culture's Ven, Octupus Card, Eagle Cash – private for U.S. army, and other local systems in E.U. and U.S.A for canteens, sport areas and library access)
- Decentralized Systems – will sell their electronic money through third party digitally exchangers (e.g. Ripple monetary system, Bitcoin, Loom)
- Offline "anonymous" systems – eCash / DigiCash ("pure anonymous"), "semi-anonymous" and based on electronic purse/wallet (not 100% electronic money) – Mondex - UK, Visa Cash – U.S, Geldkarte - Germany, Chipknip - Netherlands, Proton - Belgium, FeliCa – Japan, Moneo – France, Quick – Europay Austria, MintChip – Canada, MiniPay - Italy).

The electronic money payment systems are out of scope of this paper (because just few of them have deployments for mobile environments – see FeliCa) and the focus in these sections is on the mobile payments transactions.

No matter which model of payment service provider is adopted, there are four primary models for execution of the mobile payment transactions:

- Premium SMS based transactional payments
- Direct Mobile Billing
- Mobile web payments (HTTP vs. old WAP – with secure layers)
- Contactless – OCR (Optical Character Recognition) from images/text, NFC (Near Field Communication), NFC 2.0 or DOV – Data over Voice.

The entire process of the mobile payment may include various technologies for communications between the client and the merchant, "money transfer" and / or ticket delivery (but it is dependent by the implementation) [4] – Figure 1 and Figure 2:

- Text messaging (SMS), USSD - Unstructured Supplementary Service Data and messages through WAP Push - visual inspection or OCR
- Picture messaging (SMS, EMS, WAP Push and MMS) - usually uses a barcode – 2D barcode – QR
- Contactless – Especially for access to services provided by systems that use till now exclusively contactless ICC – Integrated Circuits Cards as NXP Philips Mifare/DESfire/JCOP, Calypso, Sony FeliCa, etc. Now the merchants are using compliant devices that exchange data through radio connection in proximity ranges with the customer mobile devices, through the device RFID embedded chipset capabilities that runs under NFC – Near Field Communication specification. A sample of NFC implementation of Mobile FeliCa (the mobile phone is in a contactless ICC emulation mode) is Japanese Osaifu-Keitai – "Wallet Mobile" a trademark of NTT DoCoMo. An alternative to radio communication are the technologies NSDT (Near Sound Data Transfer), DOV (Data Over Voice) and NFC 2.0 which produce audio signatures that allows the microphone of the mobile device to play a certain "sound" in order to trigger electronic transactions.

Fig. 1. Presenting a Data matrix 2D barcodes instead of a ticket to the validation device in a subway station – Metrorex Bucharest, Romania

Fig. 2. Presenting a DOV audio signal to the validation device in a subway station – Metrorex Bucharest, Romania

Independently by the communications methods between the customers mobile devices and the validation devices or POS, the trend in the mobile market is to provide a dedicated mobile application that runs within the smart phone OS (Google Android, Apple iOS, RIM Blackberry OS, Microsoft Windows Mobile, MeeGo – Intel Tizen, Palm OS – Garnet OS, HP WebOS – deprecated, Symbian – obsoleted but with a large number of devices in the market) or the mobile handset frameworks (JME – Java Micro Edition or .Net Compact Framework or "flavors" of them – Dalvik Java virtual machine within Android). The mobile application can store and render barcodes delivered via SMS or GSM connection GPRS/UMTS/LTE. The barcodes are rendered on the device by the dedicated application, which is especially useful for transport tickets.

3 Improvement to the Subway 2D Barcode Automatic Ticketing System – 2D BATS

The details of implementation can be obtained from the author of the paper or via web from the international conference proceedings from SECITC 2010 [8] and from the extended paper version published in [7].
The 2D BATS architecture is presented in Figure 3.

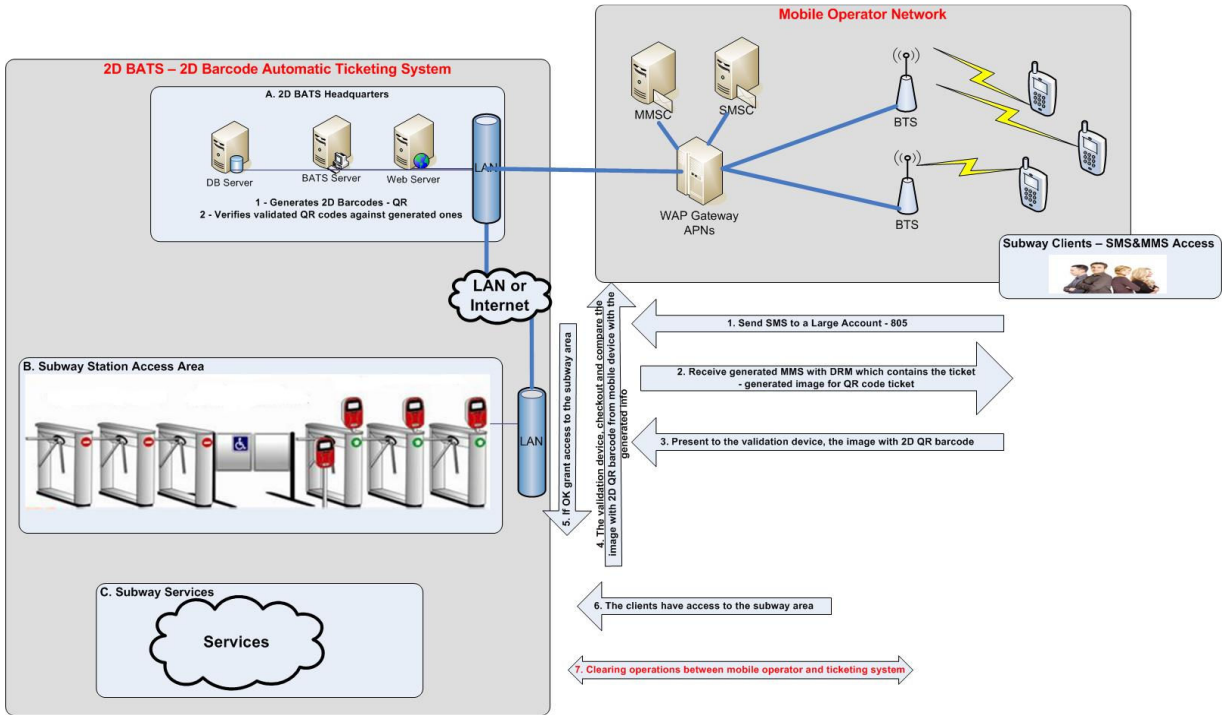

Fig. 3. 2D BATS Architecture

As an improvement to the solution from this section, it is under development a mobile JME and Android application that use web services within SOA – Service Oriented Architecture instead standard MMS with DRM – Digital Rights Management capabilities. Now, the mobile application receives encrypted ticket encapsulated within GZIPed SOAP – Simple Object Access Protocol responses. The encrypted and encoded information related to the electronic ticket is extracted from the XML message and then, it is rendered on the display as QR – Quick Response code or as Base64 text. The ticket in QR code format is presented in Figure 3.

Table 1. Text Preparation of anonymous ticket before Base64

METICKET:**N:**-;**ADR:**-;**TEL:**-;**EMAIL:**-; **ENCINFO:***Base64*(***Encrypt(line:blue;sdate:20101101Z112345;edate:20101201Z112345;nojrns:1)***);**PTSYS:**Boston Subway;**URL:** http://www.mbta.com/;

Table 2. Text Preparation of anonymous ticket after Base64

METICKET: **N:**-; **ADR:**-; **TEL:**-; **EMAIL:**-; **ENCINFO:**bGluZTpibHVlO3NkYXRlOjIwMTAxMTAxWjExMjM0NTtlZGF0ZToyMDEwMTIwMVoxMTIzNDU7bm9qcm5zOjE=;**PTSYS:** Boston Subway;**URL:** http://www.mbta.com/;

Fig. 4. QR code for one journey ticket scale 2:1

The significantly difference between the improved solution and the old one, it is the existence of a mobile dedicated application that pays the access for a special APN within the MNO bills to the provider (including prepay through the operator billing system) and also displays the encrypted and encoded electronic ticket to the mobile device display.

4 Conclusions

Summarizing, the following technologies may be used for the mobile payment service solutions:

- Short Message Service (SMS) / Multimedia Message Service (MMS) / Unstructured Supplementary Services Delivery (USSD)
- Web Applications over WAP/GPRS/3G (UMTS) & 4G (LTE) Data Connections
- Mobile Device Application (OS based: Google Android, Apple iOS, RIM Blackberry OS, Microsoft Windows Mobile, MeeGo – Intel Tizen, Palm OS – Garnet OS, HP WebOS – deprecated, Symbian – obsoleted but with a large number of devices in the market or the mobile handset cross-platform frameworks: JME – Java Micro Edition or .NET Compact Framework)
- SIM-based Application
- Near Field Communication (NFC) / NFC 2.0 – including Data over Voice.
- Dual Chip or SIM HW modified

In the future the application from section three should implement new features as NFC 2.0 and DOV – data over voice and user friendly GUI for electronic ticket management and GUI personalization.

The designers, developers and the company involved in mobile payment services should

be concerned by the technical security related to the technologies depicted above, but also with the customer trust, privacy and security in terms of social experience [15].

Parts of this paper have been presented at Advanced Study School (SSA) ''Challenges in Cyber Security – from Paradigm to Implementation" in August 2012.

References

[1] S. Karnouskos and F. Fokus, "Mobile Payment: a journey through existing procedures and standardization initiatives," *IEEE Communications Surveys and Tutorials*, Vol. 6, No. 4, 2004, pp. 44-66.

[2] A. S. Lim, *Inter-consortia battles in mobile payments standardization, Electronic Commerce Research and Applications*, 2007, doi:10.1016/ j.elerap.2007.05.003

[3] http://en.wikipedia.org/wiki/Mobile_ payment

[4] http://www.intercom.ee/mobile-ticketing-works

[5] http://en.wikipedia.org/wiki/Electronic_ money

[6] http://www.sony.net/Products/felica/ about/index.html

[7] C. Toma, "Security Issues for 2D Barcodes Ticketing Systems," Journal of Mobile, Embedded and Distributed Systems, Vol. 3, No. 1, 2011, pp. 34-53, Available at: http://www.jmeds.eu/index.php/jmeds/article/view/Security-Issues-for-2D-Barcodes-Ticketing-Systems/pdf

[8] http://www.secitc.eu – International Conference on Security for IT&C - extended papers in Journal of Mobile, Embedded and Distributed Systems – www.jmeds.eu

[9] DataMatrix 2D barcode standard ISO/IEC 16022:2006

[10] QR 2D barcode standard ISO/IEC 18004:2000

[11] H. E. Burke, *Automating Management Information Systems: Barcode Engineering and Implementation*, Thomson Learning Publishing House, ISBN 0-442-20712-3.

[12] R. C. Palmer, *The Bar Code Book*, Helmers Publishing, ISBN 0-911261-09-5.

[13] C. Toma, *Security in Software Distributed Platforms*, ASE Publishing House, Bucharest, 2008, ISBN 978-606-505-125-6

[14] Tan Jin Soon, *QR Code*, Automatic Data Capture Technical Committee Presentation

[15] M. Popa, A Calugaru, "On-line Payment System Survey – eCash," *Journal of Mobile, Embedded and Distributed Systems*, Vol. 1, No. 2, 2009, pp. 95-103, Available at: http://jmeds.eu/ index.php/jmeds/article/view/On-line-Payment-System-Survey

Cristian TOMA has graduated from the Faculty of Cybernetics, Statistics and Economic Informatics, Economic Informatics specialization, within Academy of Economic Studies Bucharest in 2003. He has graduated from the BRIE master program in 2005 and PhD. stage in 2008. In present, he is lecturer at Economic Informatics and Cybernetics Department and he is member in research structures such as ECO-INFOSOC. Since the beginning - 2005 - he is scientific secretary of IT&C Security Master Program from Academy of Economic Studies from Bucharest, www.ism.ase.ro and since 2006, he is in the editorial board of the SECITC – The International Conference on Security for Information Technology and Communications – www.secitc.eu and JMEDS – Journal of Mobile, Embedded and Distributed Systems – www.jmeds.eu. His research areas are in: distributed and parallel computing, mobile applications, smart card programming, e-business and e-payment systems, network security, computer anti-viruses and viruses, secure web technologies and computational

cryptography. He is teaching object oriented programming, data structures, distributed applications development, viruses and anti-viruses technologies, smart-cards and biometrics technologies, mobile applications systems, e-payment systems development and advanced programming languages in Department of Economic Informatics and Cybernetics – www.dice.ase.ro, and IT&C Security Master program. He has published 3 books and over 50 papers in indexed reviews and conferences proceedings.