Generic Architecture for Mobile Check System

KARIMA MAAZOUZ1
HABIB.BENLAHMER2
NACEUR.ACHTAICH3

1Analysis, Modeling and Simulation Laboratory, University Hassan 2, Morocco.
2Laboratory of Information Technology and Modeling, University Hassan 2, Morocco.
3Analysis, Modeling and Simulation Laboratory, University Hassan 2, Morocco.

Abstract

The explosion of the mobile market of Smartphone has rapidly changed the way of m-commerce transactions, especially the m-payment systems which are knowing a wide acceptance due to their diversity and the new mobile technologies. In this work we have introduced the system m-check as a mobile payment system, we have presented a generic architecture of the system and the different protocols for the implementation of the system m-check.

1. Introduction

The explosion of the market of Smartphone last years is rapidly changing the way of business transactions, Smartphone devices are driving the m-commerce market which is upset the market of e-commerce. It become a medium used to serve the customers on faster rate and at low cost[6]. It also being used to provide payment mobile in secure way[3]. The mobile payment systems are becoming new and unforeseen ways of convenience and commerce. Most of them are based on electronic payment systems[12]. There have been a several attempt to develop the electronic payment systems[1,3]. The mobile payment differ to the electronic payment by the use of new technologies[2]. The m-check or mobile check is a mobile payment system based on the idea of electronic check system[10,11], which is a dematerialized form of a paper check. The concept of e-check is initiated by Financial Services Technology Consortium(FSTC) and presented different characteristics for e-check[13,11]. Several systems e-check are proposed on literature, Net cheque[7], safe check[8], Net chex[9]. For ensure security and privacy of system e-check different methods are introduced [4,5]. The m-check is a form of e-check destined for Smartphone, it can replace paper checks without need to create a new payment instrument, it will fit into current check practices and systems with minimum impact on clients, merchants, and banks. It is compatible with technologies mobile. M-checks are better for high-valued payments, businesses to businesses payment to issue post dated check, they pass directly from client to merchant, so that the timing and the purpose of the payment is clear to the client, they have the advantage that client and merchant can be individuals, small businesses, brokerages, corporations, governments or almost any other type of organization. The rest of the paper is organized as follows. Section 2 is an overview of m-check system in which we discuss a basic concepts of m-check. In section 3 we present a generic architecture of m-check system, the protocols that describes the interactions between the users of our system. We then conclude the work in section 4.

2. M-check preliminaries:

The cycle of the m-check is based on interactions between client, merchant, merchant’s bank, client’s bank (figure1).

![figure1: M-check payment system](image-url)
An m-check system can be made on line involving the trusted party (Bank) or offline without the use of bilateral agreements or additional communication. An m-check written on XML can be send in different ways using mobile technologies Bluetooth, NFC, or by a sample mail.

**Entities of system m-check:** the entities involved in the m-check system resemble the entities in e-check systems based on a paper check system: client is the entity who wishes to make payment with m-check to another entity. Merchant is an entity who the m-check is addressed to. Merchant’s bank, client’s bank, certification authority (AC) which can be a bank itself.

**Processing information:** Each m-check should contain specified and familiar check information like: m-checkID (unique identifying m-check number), unique account number, a unique issuing bank identifier, the date, the amount and the currency of payment. An m-check can contain some optional information like the Bank’s name and address, the certificate number.

**M-check payment process:** The client writes the m-check using the options legally required to be in a check in his check-book mobile (m-checkbook), sign it cryptographically and send it to the merchant. Thus the m-check is retired from the Smartphone device of the client. The merchant receive the m-check and stock it in his m-checkbook, he can deposit it in his bank to time. If the client and merchant have the same bank, the bank accept the m-check, verifies their signatures update the client’s account by withdrawing the check amount, and inform the depositor about its status or return the m-check. Credit the merchant’s account and debit the client’s account. If client and merchant have different banks, the merchant’s bank verifies the signature of merchant, credit his account and forward the m-check for clearing and settlement, the client’s bank verifies the signature of his client and if this m-check is not a duplicate, then debit his account. Therefore the client receives a line item on his statement contain a description of the transaction. To ensure security each member in the payment scenario should authenticate before committing the payment. It’s assumed that client and merchant are registered as users with the m-check system and both of them have a valid digital certificate.

**Description of the m-checkbook:** the m-checkbook is an application based on the privacy of SIM card, loaded into the Smartphone of the client system m-check, provided by the bank if asked. The application contain a define number of m-checks which can be used by the client any time. The application is unlocked by a PIN number editable by the client if need (to ensure the security of the application). The m-checkbook contain an m-check register to be consulted later. In case the Smartphone is lost, the client can give a stop payment request to his bank for remaining m-checks and the request can be made for a new m-checkbook.

**3. M-check system architecture:**

The system consist of five phases: (a) system set up during which the client obtain a digital identity. (b) registration of clients in which the client obtain the m-checkbook digitally signed by the bank. (c) m-check write protocol in which the client write and sign an m-check that contain all necessary information. (d) a deposit protocol during which the merchant make a deposit of the m-check with his bank. (e) a payment protocol in which the bank treat the m-check.

we are describing the scenarios of interactions between client merchant and bank in the case of payment of services and good under the m-commerce transactions. an m-check also can be exchanged between any two client of the m-check system.

**System set up:** in this phase each user of our system m-check must obtain a digital identity. The following messages are exchanged between the client and the certification authority (CA) for obtaining a digital certificate:

1. the client send certificate request containing his information to the CA.
2. CA receive the request compile it and sign it using his private key.
3. the digital certificate (DC) is installed at the client side.

The certification authority which is responsible for issuing and revoking digital certificates, may itself be the Bank of the client.
Registration protocol: The client (client/merchant) must register his identity in his bank to get his m-checkbook. The following messages are exchanged for the issue of the m-checkbook:

(i). the client connect to his bank.
(ii). the bank accept the connection request.
(iii). the client and the bank exchange their digital certificates.
(iv). the client request the bank by providing his account details for the issuing of the m-checkbook.
(v). the bank validates the details in the request, and send the m-checkbook.

M-check write protocol: any two client can exchange any number of m-check as follows:

(i). the client and merchant exchange their digital certificates.
(ii). the client and merchant exchange the m-businesses data.
(iii). the client writes the m-check, sign it and send it to the merchant.

M-check deposit protocol: the merchant can deposit an m-check with his bank as follow:

(i). The client connect to his bank.
(ii). The client deposit the signed m-check in his bank.
(iii). the bank receive the m-check, verifies signature and valid the information about the depositor.
(iv). The bank send confirmation to the merchant.

\[ \text{1) Merchant} \quad \text{Signed M-check} \quad \text{Bank} \]
\[ \text{2) Merchant} \quad \text{Confirmation} \quad \text{Bank} \]

M-check payment protocol: once the m-check is deposited with the bank the following messages are exchanged. (we discuss the case the client and merchant has the same bank):

(i). The bank verifies the certificates and signatures of the received m-check, validate the account information.
(ii). The account of merchant is debited and that the client is credited.
(iii). The bank send a confirmation messages to their clients.

In the case the bank of client is not the bank of merchant, the merchant deposit the m-check in his bank, the merchant’s bank send the m-check to the client’s bank for clearing and settlement operation.

\[ \text{1) Bank} \quad \text{Verify Information} \quad \text{Confirmation} \quad \text{Client/Merchant} \]

Client and merchant system/Bank Servers:
Client and merchant systems are used to write m-checks, verify signatures, provide interfaces and prepare deposits for transmission to the banks. Servers m-check system in banks are used to receive m-checks and process them. The modules regrouped in client and merchant system and bank servers are:

- Certificate server/m-check issue: certificate renewal, and process m-check issue, and stop payment requests.
- M-check writing: this module contain the operation of writing and deposit processing m-check.
- M-check and attachment verification: include the verification of the m-check signatures and validate certificates.
- M-check payment: handles the operation of payment and avoid the duplicate payment.
- Interfaces: provides the mechanized interfaces to the user’s accounting system and m-check, and interfaces between the bank operational systems and m-check systems.
- M-check register/archival system: contain record of m-checks written by the client and all paid m-checks.

4. Conclusion

Smartphone devices are becoming very important for m-commerce. In this paper we presented the m-check as mobile payment system which aims to ensure security, interoperability, and universality. The m-check which is considered like financial document will reduce financial transaction overhead costs enable new m-commerce and m-banking services.

References:


[7] Neuman B Clifford, Medvinsky, Gennady , Net cheque Net cash and the Characteristics of Internet Payment Services, the journal of electronic publishing, Volume 1, Issue 1&2, 1995


