Mobile Financial Services

Telecom Regulatory Authority of India (TRAI)

Issues for Consultation

www.gemalto.com

Table of Contents

1 Introduction

A comprehensive suite of secured mobile financial services, enabling online transaction management via any mobile, web or other access channel is essential for stabling a successful mobile financial services ecosystem.

By equipping mobile network operators and service providers with the technology and know-how to manage these kinds of services, mobile financial services vendors enable the creation of an effective MFS ecosystem.

In the following document Gemalto will share his view on services and requirements that should best fit with Indian market. The MFS technology will be presented as MFSSP (Mobile Financial Secure Service Platform). This platform could ultimately be Gemalto Platform but remains a generic wording in the document.

The Gemalto solution is called the TRIV Platform™, is based on a powerful server-based solution that delivers a user experience tailored to customer needs. Unlike common mobile wallet solutions that only provide a single stored value account or a connection to a single account, Gemalto offers a real-life wallet experience, bundling together multiple payment methods, such as bank accounts, credit/debit cards, stored value and telecom accounts. Moreover, the user can flexibly move funds between different “pockets” in the Gemalto account, which can be accessed from both mobile and non-mobile environments.

2 Issues for Consultations

2.1 What method(s) of communication on mobile network (GSM and CDMA) would be suitable for enabling financial transactions using mobile phones? Please explain your answer

End-to-End Security is essential for any mobile financial services with powerful transaction management.
A superior user experience is possible, with no security trade-off. A Secure Mobile Financial Services is needed to secure all communication between the mobile front-end to the back-end financial processing and back office cluster. A secure channel is established between the SIM card, the secure element executing the client application and holding the transactional keys, and the HSM, which holds the keys on the server side.

Any message from end user mobile until the Bank Switch or Store Value account has to be End to end encrypted.

Encrypted SMS using Dynamic Sim Tool Kit is the most suitable Method of communication for security and user experience. This solution is SIM client-Server based solution. Second and alternative solution could be handset client – Server solution but still with End to end encrypted message.

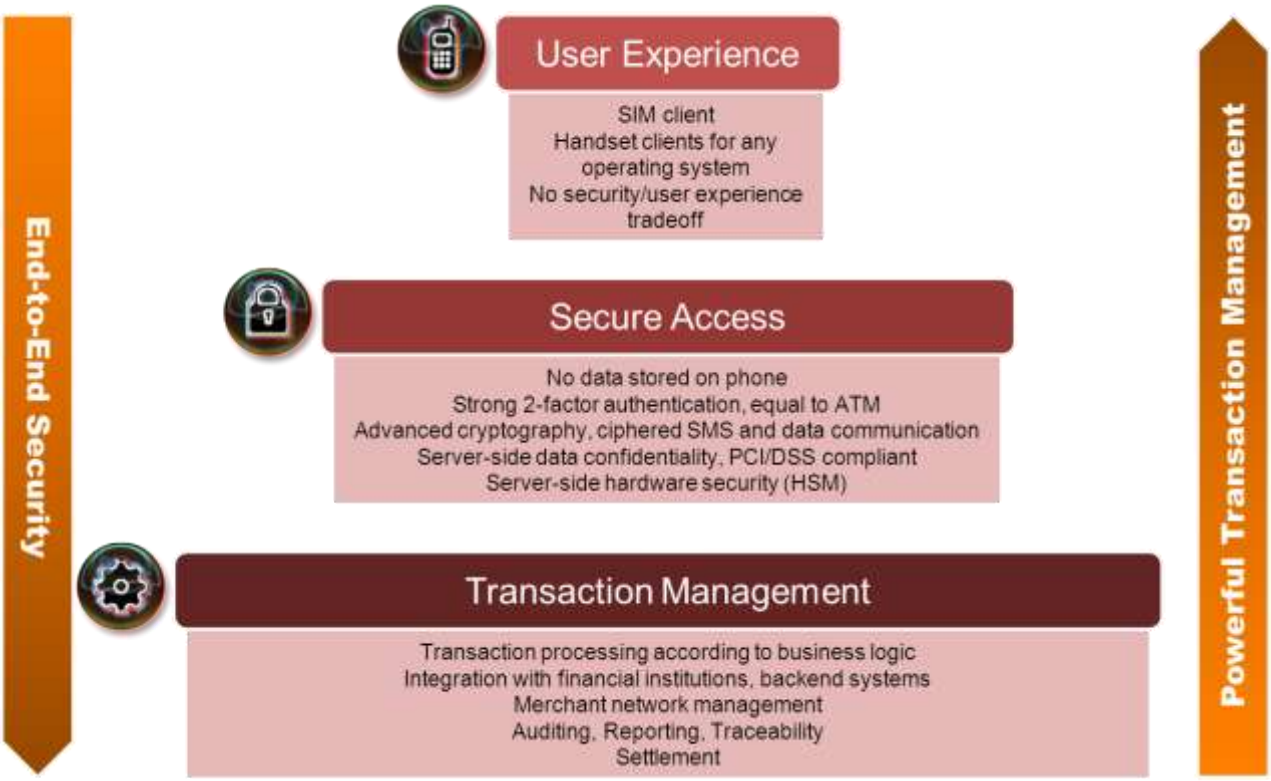
A key factor in the adoption of any new service is the user experience. A good user experience will encourage trial and use. For new recipients of transfers, receiving the right message to easily register will encourage uptake. The Mobile Financial Services Platform should offer multiple methods to access services, each with its own intuitive and easy to use interface. As the wallet itself is stored on the Mobile Financial Services Platform, it can be accessed using any method convenient to the customer at any given time. The services are accessible from the handset itself, the internet, Point of sale, ATM machines, IVRs, and more. The extent of the flexibility allows accessing the mobile wallet by means of SMS, USSD or handset applications such as SIM tool kits or J2ME applications, WAP, and Points of Sale via backbone integration to merchant POS networks.

End-to-End Security

The MFS vendor as Gemalto has to provide the industry's leading Mobile Financial Services solution with end-to-end security and powerful transaction management. A superior user experience is possible, with no security trade-off.

The Mobile financial Services Secure Platform (MFSSP) secures all communication between the mobile front-end to the back-end financial processing and back office cluster. A secure channel is established

between the SIM card, the secure element executing the client application and holding the transactional keys, and the HSM, which holds the keys on the server side.



On the mobile front end, users are required to identify themselves with a PIN, which protects access to financial information and transactions. Secret keys only known to the SIM card and the service provider are used to encrypt and sign transaction data, further proving the identity of the user.

The Secure Mobile Financial Service Platform should go far beyond standard telecom security:

- Strong two-factor authentication is provided by the SIM and PIN. Users are required to identify themselves with a PIN that protects access to financial information and transactions. The PIN is encrypted in the SIM and never decrypted. Secret keys only known to the SIM card and the server are used to encrypt and sign transaction data, further proving the identity of the user.
- Data is classified and ciphered separately.
- The secure execution environment of the SIM provides signature facilities and non-repudiation assurance.
- Additional protection is achieved by using a different key for each transaction (Derived Unique Key Per Transaction (DUKPT) standard).

- The cryptographic functions, including key management, are performed using the most fraud-resistant hardware solution. Both the SIM and server-side Hardware Security Module are certified as complying with the most stringent security standard: FIPS 140-3 Level 3. The Hardware Security Module itself uses a proprietary mobile financial services firmware that reduces liability and risk.
- Secure OTP (One Time Password) generation and validation using the HSM.
- Anti-phishing mechanisms.

2.2 What in your view would be appropriate time frames for delivery of messages and responses with respect to the method(s) suggested by you? What parameters need to be defined to ensure timely delivery of information to support financial transactions using mobile?

The TRIV™ Platform is agnostic to any access channel (STK, UTK, SMS, J2ME, ATM, POS, API, etc). The appropriate time frames for delivery messages depend highly on the requested user experience, access channel, type of MFS Service Flow, and country where the service is delivered.

The SMSC is responsible of delivery of SMS messages. The TRIV Platform™ is not responsible of sending the MFS related messages with a high priority but can add a **tag** to any MFS message string to the SMSC from the TRIV Platform™. Based on this tag the SMSC (if supported) can prioritize the MFS SMS.

The system supports time outs and can support retry – mechanism if periphery systems (bank systems, prepaid system) are not responding. After a certain time out the transaction is failed.

Further the system supports non interactive and interactive flows.

2.3 In the method suggested by you would it be possible to prioritize the transaction messages over other messages on the network? If yes what would be the cost implications? Please also reply this with reference to SMS as means for financial transactions.

As indicated in 2.2, The TRIV Platform™ is not responsible of sending the MFS related messages with a high priority but can add a **tag** to any MFS message string to the SMSC from the TRIV Platform™. Hence, the SMSC need to be supported to prioritize the MFS SMS

The cost implication could be minor from MFS vendor in adding additional tag to the MFS message, but more on the SMSC to support this prioritization.

2.4 What do you think would be the security requirement using the method proposed by you for the five basic transactions i.e. no-frills account opening, cash in, cash out, checking balance, and money transfer?

System Security

The Mobile Financial Services Secure Platform is a highly secure payment processing system, designed to address all aspects of payment security. These include end-user privacy, non-repudiation and administrative privileges. Gemalto implements and supports effective security concepts and enables the use of industry-leading security techniques.

Information Security

MFS vendor technology as Gemalto has to ensure end-to-end security by ciphering messages exchanged between the SIM or any handset client and the bank or Mwallet system using the highest existing security standards.

In the following description, to ease the reading of the document, Financial Institution, bank or PSP via mwallet platform is commonly called “Bank” as the security concept should be similar for banked or unbanked people.

We recommend SIM client based solution as the following:

Special keys are embedded permanently in the SIM at manufacturing so it is not possible for anybody to duplicate them. All sensitive data is kept exclusively at the bank or in dedicated environment of the MNO when PSP.

The cryptographic keys used to secure financial transactions are under the sole control of the bank. They are managed using the most tamper-resistant hardware solution: a Host Security Module device compliant with the FIPS 140-2 level 3 security standard.

The MFSSP technology, as Gemalto one, must guarantees that even if one of the components of Mobile Banking is compromised, the overall security is not affected.

Secure Data Transfer

For the highest level of security, sensitive data, such as PIN and transaction details are never stored in the SIM or the platform. All customer and financial information is kept exclusively at the bank, which also has the sole control over the cryptographic keys used to secure financial transactions.

Strong 2-factor Authentication

End user must be sure that nobody can make transactions on their behalf and banks or PSP must be able to verify that the end user customers are those who they claim to be. MFSSP as Gemalto technology responds to this requirement with strong 2-factor authentication.

Data Integrity

Since data is digitally signed, any attempt to manipulate it will be detected because the signature will no longer correspond to the signed message.

Non-repudiation

In the context of mobile banking, non-repudiation refers to authenticating the customer and the financial institution participating in a financial transaction with high degree of certainty so that the parties cannot later deny having performed the transaction. To ensure non-repudiation, a proof must be generated that the transaction was performed by that party.

MFSSP addresses this requirement through the use of:

- A user PIN known only to the user and protected by encryption
- A transaction confirmation code sent by the bank
- A transaction log that records the details of every transaction

Cryptographic Operations

All sensitive data is encrypted with double length 3DES keys (128bit keys). In addition, transactional security standards such as Derived Unique Key Per Transaction (DUKPT), short-lived transactional contexts and key roles are used for added protection of financial transactions.

The cryptographic functions, including key management, are performed using the most fraud-resistant, hardware solution: a Host Security Module augmented by Gemalto's firmware, which personalizes the HSM

for Mobile Banking. The selected HSM by Gemalto is certified to the most stringent security standard: FIPS 140-2 Level 3.

Host Security Module

The Host Security Module (HSM), a tamper-proof hardware component located at the bank (could be at PSP premises), provides state-of-the-art cryptographic functions to the MFFSP gateway and safeguards the cryptographic keys used to secure the financial transactions processed through the MFFSP gateway. This has to be certified to FIPS 140-2 Level 3.

Secure application

The SIM card, a tamper-resistant smart card includes an application (an applet) with an intuitive user interface and security features that ensure the same level of safety and confidentiality as if the operations were performed at the bank.

This application is written in Javacard so that can be portable and interoperable on any Javacard and supported by most Handset of the market.

The Secure Applet, pre-installed in the SIM card and thus readily available to the end-user:

- Displays the appropriate menus and gets the user responses
- Sends and receives transaction messages
- Encrypts and decrypts sensitive information
- Manages the security and confidentiality of the transactions

2.5 What would be measurable QoS parameters for such networks? Please specify both network and customer centric parameters.

Monitoring and Tracing

Built on market standard infrastructure components, the MFSSP offers the best monitoring and tracing management tools.

Monitoring and Control

A lot of the monitoring and control is performed via the application server's provided mechanisms. The application server can be controlled using the application server console.

Upon request, as MFS vendor as Gemalto can provide a dedicated monitoring server based system. It uses a large number of available plug-ins to detect the health of the components of the platform and report it via a web interface or using email and SMS. As part of this solution Gemalto also deploys in-house developed monitoring plug-ins that detects multiple MFSSP specific parameters, which are also reported via specific interfaces.

Logging and tracing

All MFSSP activity is logged into log files. Log messages are assigned a severity level.

In a production deployment, the MFSSP logger is usually configured to log messages at the Info, Warning and Error severity levels. When required, the logger can be configured to enable or disable logging of any severity level per application component (for example: enable Debug messages for purchase processes).

Data and Reporting

The platform offers several mechanisms to allow access to payment related data.

2.6 Please list any other issue that you think is important and your comment thereon to finalise QoS parameters for facilitating financial transactions on mobile network?

There are several other parameters, which are not noticeable in facilitating financial transaction on mobile network. However, it is part of the entire transaction and should not be neglected.

Self-Care Applications

The MFSSP features comprehensive business management tools for administrators, merchants, distributors, agents and customers, enabling them to manage their accounts and activities and view transactions and history.

Administrative Application

Administrators have the highest authority within the system, and as such can perform a wide range of operations according to their individual permissions.

The Administrative Application is web-based software used by two main functions:

- Customer Care agents, who assist customers with registration for services and the creation of pockets, as well as helping them perform or resolve transactions.
- System Administrators, who have overall responsibility for the system configuration, and who define risks and limits, register pocket issuers and bill issuers, generate reports, etc.

Within this application, users have role-based access, which limits their activity to a subset of relevant permissions.

Merchant Self-Care

The Merchant Self-Care application is used by the organizations and individuals who distribute and sell goods and services in the MFS ecosystem. Administrators log in to create and manage the merchants and distribution networks.

Customer Self-Care

The Customer Self-Care application is web-based software that allows customers to register for the service, add and modify pockets, perform transactions, check their balance, and view their short-term transaction history. It provides a rich online user experience equivalent to the handset options and with several additional capabilities

3 Conclusion

The highly scalable and unique architecture of the Mobile Financial Services platform is especially suited for large global operators and service providers who wish to manage multiple and interoperable payment networks and commerce eco-systems worldwide.

Gemalto has global partnerships in the telecom and banking industries and has already performed numerous integrations with leading billing and pre-paid systems, banks and clearing gateways.

Gemalto, with numerous deployments around the world in both emerging and developed markets, understands the needs of operators and service providers, providing timely, cost effective and flexible deployments.

For More details pls. Contact:

Arbind Kumar Sinha

Email:Arbind.sinha@gemalto.com

Mobile: 98917 46930

Gemalto Digital Security Ltd

Lotus Tower, New Friends colony

New Delhi-110065

End of document-