Mobile Banking

Product Overview

FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS > PRODUCT

TRANSPORT

gemalto
security to be free

Introduction

Mobile phones have become an integral part of the 21st century landscape with an expected penetration of 4.5 billion by 2011. While North America and Europe have the highest penetration rates, reaching 100% in many Western countries, South America and Asia represent the fastest growing mobile markets.

In developing countries, the role of the mobile phone is more extensive than in developed countries, as it helps bridge the digital divide. Even with initiatives like the OLPC, the penetration of the PC lags far behind that of the mobile phone.

The mobile phone is the one device that people already carry at all times, and services beyond voice and text messaging are booming all over the globe. Users want the same kind of services for their mobile phone that they can get through an Internet-connected PC. But cost is an important factor, as new services will be widely adopted, but pricing must be carefully considered, since Internet users have come to view the service as free.

People living in emerging markets or remote regions of Africa, South America and Asia who don't have a bank account or a computer still often own a mobile phone, which can provide them with access to basic financial services. Mobile phones represent a cost-effective solution for users, financial institutions and operators, allowing them to bridge the digital divide in places where traditional banking and Internet services are too expensive or simply nonexistent.

Easy access to financial services is widely accepted as a good thing: users have access to credit and can securely manage their money, financial institutions expand their user base and process more transactions, and governments benefit from the effect credit has on lower-income sectors of the population and can better track funds distribution within their country.

Ubiquitous and versatile, wireless devices can give users easy, 24/7, access to financial services bringing the next market revolution - mobile banking, mobile payment, mobile wallet, mobile money transfer and other financial services - to users everywhere. Indeed, while the rate of Internet banking user growth has stabilized, mobile banking is spiking and market analyses say that more than 800 million people will use the service by 2011.

The dramatic increase in mobile phone usage has been followed by an increase in mobile fraud, and although eager to use mobile financial services, many subscribers are concerned about the security aspect when carrying out financial transactions over the mobile network. In fact, lack of security is seen as the biggest deterrent to the widespread adoption of mobile financial services. Internet transactions suffer from the same problem, as do traditional payment transactions… fraud prevention has become a pressing need across all modes of financial transactions.

Gemalto has responded to these needs by developing the most secure Mobile Banking solution on the market. It provides a comprehensive set of financial services: alongside full mobile banking and security features, Gemalto Mobile Banking offers a wide range of payment options such as prepaid airtime purchase, bill payment, credit advance and others. Wireless operators and financial institutions can now offer their customers the freedom to manage their finances whenever and wherever they want, without being concerned about security and confidentiality issues.

Gemalto Mobile Banking is designed to integrate easily with the existing mobile network and banking infrastructure while opening up new business opportunities for mobile operators and financial institutions, and providing a foundation for new cost-effective services and revenue opportunities.

Part 1 Product Description

Gemalto, a world leader in digital security, does not compromise security for convenience; we offer both. Our Mobile Banking solution provides a full range of secure and easy-to-use banking and payment options available directly from a mobile phone.

The Gemalto Offer

The Gemalto Mobile Banking offer is a complete financial services solution for mobile operators and financial institutions. It includes a secure SIM applet and a distributed transactional platform that provide secure access from a mobile phone to mobile banking, mobile payment and mobile money transfer services.

The Secure Applet is pre-installed on the SIM card, readily available to the end-user. This applet handles:

- Displaying appropriate menus processing user responses
- Sending and receiving transaction messages
- Encrypting and decrypting sensitive information
- Managing transaction security and confidentiality.

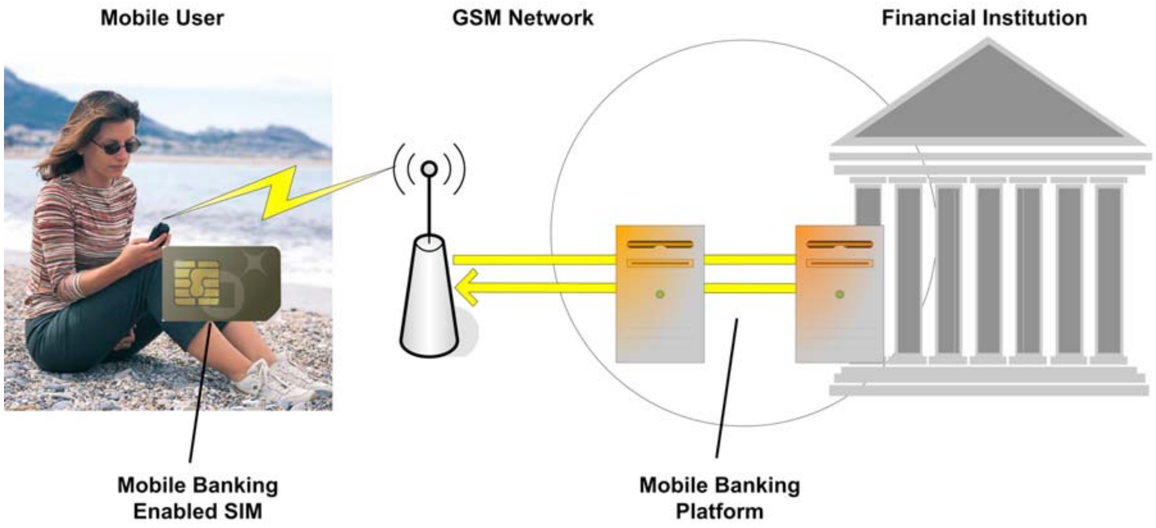


Figure 1: Mobile Banking Overview

The Distributed Transaction Platform deployed both at the mobile operator's site and at the financial institution securely manages financial operations carried out between the mobile user and the bank, over the wireless network.

Specifically, this platform:

- Maintains communication between the SIM card and the financial institution
- Routes mobile banking messages
- Manages mobile banking sessions
- Securely handles sensitive information
- Ensures the confidentiality and security of mobile transactions
- Manages user information
- Authenticates users.

Gemalto offers a customizable, end-to-end, comprehensive and secure Mobile Banking solution with the lowest entry barriers.

Low entry barriers
Gemalto technology does not rely on data communications, which are both expensive for users and complicated to configure properly, nor does it require any installation or configuration steps on the part of the end user. The mobile banking solution already resides on the user's mobile phone, as an applet on the SIM card, and therefore users do not need to download or install anything.

Comprehensive

Alongside full mobile banking and security features, Gemalto Mobile Banking offers a wide range of payment options such as prepaid airtime purchase, bill payment, and credit line authorizations.

Secure

The end-to-end security of Mobile Banking is ensured by Gemalto's state-of-the-art secure technology featuring:

- A tamper-resistant SIM card
- OS logical security protecting the SIM from unauthorized operations
- A tamper-resistant cryptographic module
- Gemalto's firmware for secure transactions
- Adherence to financial and security industry standards and best practices.

With Gemalto's secure platforms, sensitive information is ciphered at the SIM level for secure transfer over the GSM network using the highest existing security standards, and the cryptographic operations are carried out using the most fraud-resistant hardware solution (FIPS.

Mobile Banking security features include strong two-factor authentication, non-repudiation, data confidentiality and data integrity.

Customizable

Gemalto's product is customizable, allowing financial institutions and mobile operators to offer branded services tailored to customers' requirements and needs.

- Does your bank require an additional security code for certain financial transactions or wish to restrict fund transfer to local accounts?
- Do you want mobile banking to integrate seamlessly with the other services you are offering?
- Do you want to offer a new service through the Mobile Banking channel?

Our experts will work with you in order to tailor a Mobile Banking solution that corresponds to your needs.

Mobile User Experience

Gemalto Mobile Banking provides mobile users with easy and secure access to financial operations from their mobile phones 24 hours a day, 7 days a week.

Service Overview

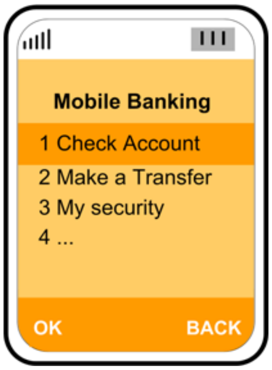
Whether they need to pay a bill while away from home, to check their account balance at the supermarket, to transfer funds on the way to the airport, to recharge their prepaid mobile subscription account before going to the beach or to obtain credit online for that new TV, mobile users can pick up the phone and carry out the desired transaction by hitting a few keys.

They simply need to browse user-friendly menus and respond to service prompts. The information they need to enter has been scaled down to a minimum, in order to simplify the use of the application. This information mainly consists of their PIN and the amount of money involved in the transaction.

A message summarizing the user's request is then sent to the selected financial institution, where the request is processed. The result is displayed on the user's mobile screen within seconds.

Service Features

With Gemalto Mobile Banking mobile users can perform the following banking operations:



- Subscribe to the mobile banking service at their financial institution, and cancel their subscription at any time
- Add or remove a bank account from a list of available accounts managed through mobile banking
- Simulate transactions in order to try the system
- Verify the balance of their bank accounts
- View the most recent transactions on their bank accounts
- accounts managed through mobile banking
- Apply for and pay off a credit line
- Check the amount of credit available on their credit cards
- Obtain cash advances on their credit cards
- Check the balance of their credit card accounts
- Pay their credit card account
- Recharge their pre-paid mobile accounts
- Pay utility bills, such as electricity, Internet and mobile subscriptions, or any other bill that can be registered with the financial institution
- Pay other services through reference numbers found on the bills.

- Add or remove a credit card account form the list of available Transfer funds between different accounts
- Transfer funds between different accounts including to another customer’s account, or an account in a different bank
- Mobile Wallet (stored value account)

Benefits

Mobile phone operators and financial institutions will benefit from using Gemalto Mobile Banking to offer mobile financial services to their customers, whether they operate in saturated markets where competition is tight and service differentiation is key to attracting and retaining customers, or in remote areas in need of cost-effective financial services.

Benefits for Mobile Operators

With Mobile Banking, operators can expand their services portfolio, promote their brands and create strategic marketing differentiation - attracting new customers.

Subscribers who use mobile financial services begin to rely on them, making them a differentiating factor for the operator. As a result, Mobile Banking strengthens customer loyalty and reduces churn and attrition rates.

Mobile Banking increases operator revenue by boosting traffic and providing subscribers with instant access to airtime purchase: with financial services at their fingertips, mobile users will recharge their pre-paid accounts more readily and use their mobile phones to pay bills or check their account balance.

Thanks to the ubiquity and high penetration of the mobile device, mobile operators are uniquely positioned to play an important role in the expanding mobile money transfer and mobile payments markets.

Benefits for Financial Institutions

Mobile Banking allows financial institutions to enhance customer satisfaction and retention by offering new, better services while gaining a direct marketing channel for their products and services, which can be tailored to the specific needs of customers. At the same time, they attract new customers to the one-on-one bank-customer relationship.

As access to mobile phones grows worldwide, so does the opportunity to attract more customers and extend the reach of financial services. By turning mobile phones into their bank’s ATMs, financial institutions gain access to new markets, different from those traditionally served by their physical branches.

Access to banking services at anytime and from anywhere also generates revenue through higher service usage, and reduces operating expenses because of fewer direct teller interactions, while maintaining or improving the level of service.

Financial institutions gain another important benefit by adding Mobile Banking to their existing channels. They will be with their customers at all times, ready to help them, to recharge a pre-paid mobile phone on a Saturday night, to get a new MP3 player via online credit funds, to pay a forgotten bill after leaving for a vacation, to transfer money to a spouse when at work - the bank is everywhere, all the time.

.

Benefits for the End User

The mobile banking application:

- Provides state of the art security
- Requires no configuration
- Is readily available
- Is low cost (no data connection) it’s resides on the SIM, the browsing is local.
- Is device independent, supported on ALL phones from low to high-end

Part 2 Technical Description

In designing and developing Mobile Banking, Gemalto has leveraged its experience in digital security and its knowledge of financial, commercial and telecommunications digital environments to create a solution that combines ease of use, efficiency, and security. Gemalto has used open GUIs and followed established industry standards and practices to facilitate integration and counter fraud. Gemalto Mobile Banking is a secure and flexible solution.

High-level Architecture

Mobile Banking Components

Gemalto Mobile Banking is enabled in the mobile phone through a secure applet located in the end-user's SIM card. Secure transfers over the wireless network and financial transaction processing are managed by the SIM card and a distributed platform, deployed at the mobile operator's site and at the financial institution. The platform includes the following components: the Business Mediation Server, the Bank Secure Platform and the Host Security Module. Additionally, an adaptor may be required to enable communication over non-standard interfaces to bank systems.

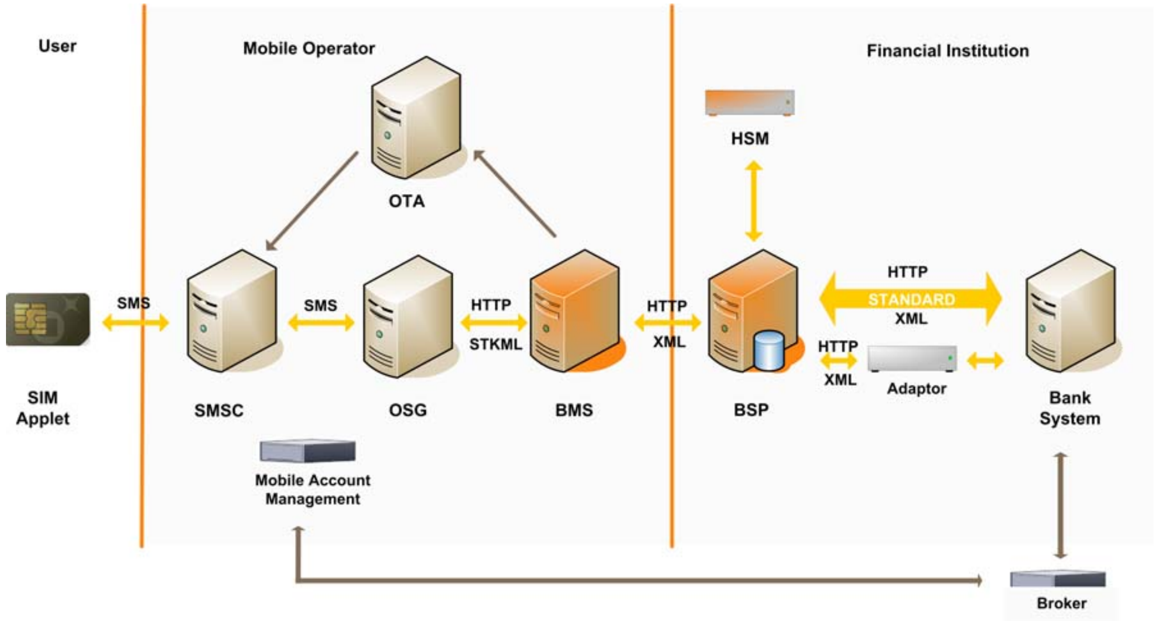


Figure 2: Mobile Banking Architecture

Secure SIM card Applet The SIM card includes an applet with an intuitive GUI and security features that ensure the same level of security and confidentiality as if the operations were performed at the bank. The applet:

- Formats and displays mobile banking menus and data
- Prompts the user for information and collects user input
- Generates transaction keys, ciphers sensitive information and signs data to be sent
- Provides the means for key management
- Sends banking requests using SMS messages.

Business Mediation Server (BMS) On the operator's side, the BMS ensures communication between mobile subscribers and financial institutions, and routes mobile banking transactions exchanged between the SIM card in the mobile user's phone and the BSP at the user's bank. The BMS:

- Receives subscribers' mobile banking requests, interprets them, formats and forward the requests to the subscribers' bank for processing
- Maintains the status of the requests
- Logs transaction results for auditing and billing purposes
- Receives the bank's responses and sends them to the SIM, via LinqUs OSG
- Maintains the list of financial institutions available on that operator's services.

Bank Secure Platform (BSP) On the financial institution side, the BSP handles transactions between mobile users and the bank's systems. More specifically, the BSP:

- Facilitates communication between bank systems and end-users
- Hosts response templates (pages)
- Authenticates mobile customers
- Maintains connectivity between the wireless telecom world and the banking environment
- Ensures that financial transactions and customer data are secure, using the services of the Host Security Module,

Host Security Module (HSM) The HSM, a tamper-proof hardware component, provides state-of-the-art cryptographic functions to the BSP. Upon receiving a request from the BSP, it performs cryptographic operations, generating transaction keys, encrypting and decrypting sensitive information. The HSM also manages the cryptographic keys used to secure mobile financial transactions. The HSM is further enhanced with the Mobile Shield firmware for secure business transactions.

Adaptor The Adaptor, required only when non-standard interfaces to the bank systems are used, is a customizable module that translates messages to and from the format used by the bank's back-end. The Adaptor seamlessly insulates the BSP from the specifics of the bank systems' interfaces.

Several operator-owned modules also participate in delivering the Mobile Banking functionalities:

- LinqUs Online Service Gateway (OSG) helps operators to offer SIM card-based services to their subscribers by connecting them to remote content in a session mode. In the context of mobile banking, OSG relays mobile banking messages between the mobile phone and the BMS and translates them from SMS to HTTP format.
- LinqUs Over-The-Air (OTA) Manager is an optional component that offers operators the convenience of remotely provisioning and managing SIM cards.
- A Short Message Service Center (SMSC), a standard GSM network element, delivers SMS messages.

Interfaces and Protocols

Mobile Banking components use standard protocols and interfaces to exchange information and to communicate with other network elements and bank systems, thus facilitating the integration of Mobile Banking into the existing infrastructure.

A high-level view of the protocols used to exchange messages between different mobile banking, operator and bank components to process a request is as follows:

- The SIM card sends Mobile Banking requests using SMS (S@T protocol) messages.
- OSG translates these messages into HTTP requests before sending them to the BMS.
- The BMS forwards the HTTP requests to the BSP of the selected bank.
- The BSP interacts with the HSM for the cryptographic operations.
- The BSP communicates with the bank's systems, possibly through an adaptor, using a series of web services.
- The bank system (or adaptor) responds.
- BSP ciphers the necessary information (using the HSM) before proceeding.
- The BSP forwards and formats the response and then sends it to the BMS
- The BMS sends the response to the OSG.
- OSG compiles the response and sends it to the SIM using the SMS channel.

Network Configuration

With Gemalto Mobile Banking, an operator can provide the service to subscribers that have bank accounts with different financial institutions. A bank can also choose to work with several operators, to provide mobile banking services to its customers, independently of their mobile service provider. It is also possible for several banks with light mobile banking traffic to share a Bank Secure Platform.

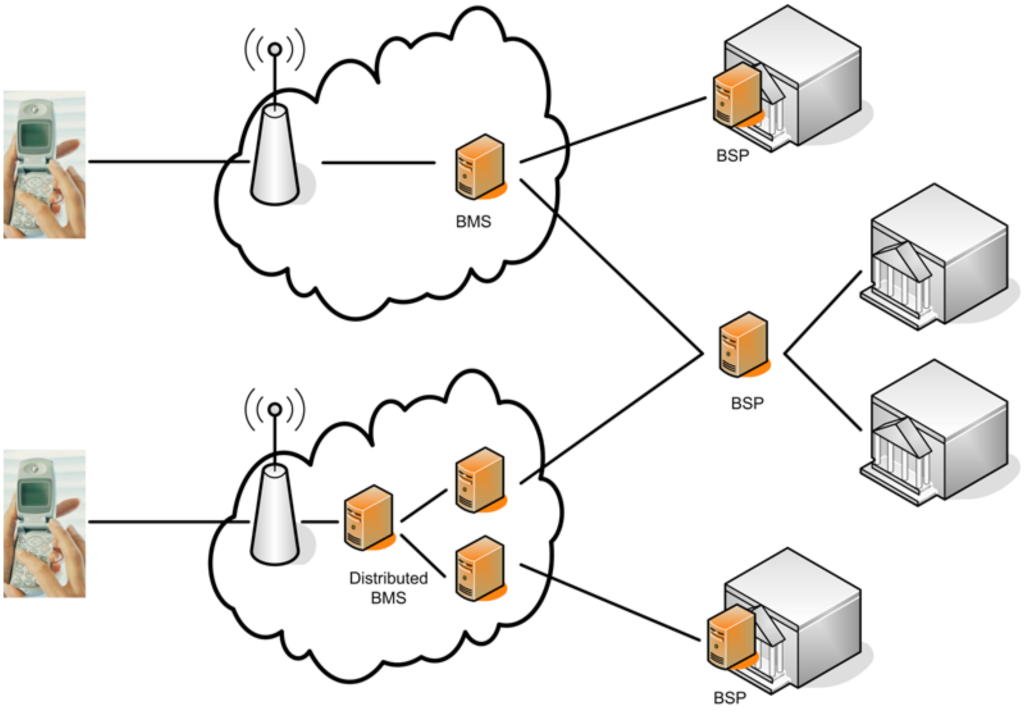


Figure 3: Network Configuration

Scalability

Mobile Banking is scalable through hardware clustering. To increase throughput, both BMS and BSP can (independently) be installed in clusters with a clustering engine distributing the traffic among several servers.

End-to-end Security

Since mobile banking transactions can be initiated from almost anywhere and transaction details are transmitted over unprotected networks, security poses the biggest challenge in developing a successful solution and is likely to be a make-it-or-break-it factor for mobile banking.

Gemalto takes security issues and concerns seriously. As long-time leader in digital security, Gemalto uses the state-of-the-art security technology to secure mobile applications.

The Mobile Banking solution addresses the requirements of data confidentiality, strong user authentication, data integrity as well as non-repudiation, and conforms to relevant standards (such as PCI DSS) established by financial organizations and government bodies to prevent fraud and other security threats.

Security and Confidentiality of Information

The Mobile Banking solution provides end-to-end security and confidentiality of data by ciphering information in the SIM for secure transfer over the mobile phone, the GSM network, the operator's infrastructure and the connection to the financial institution. The information entered by the user is collected and encrypted by the applet residing in the tamper-proof SIM card.

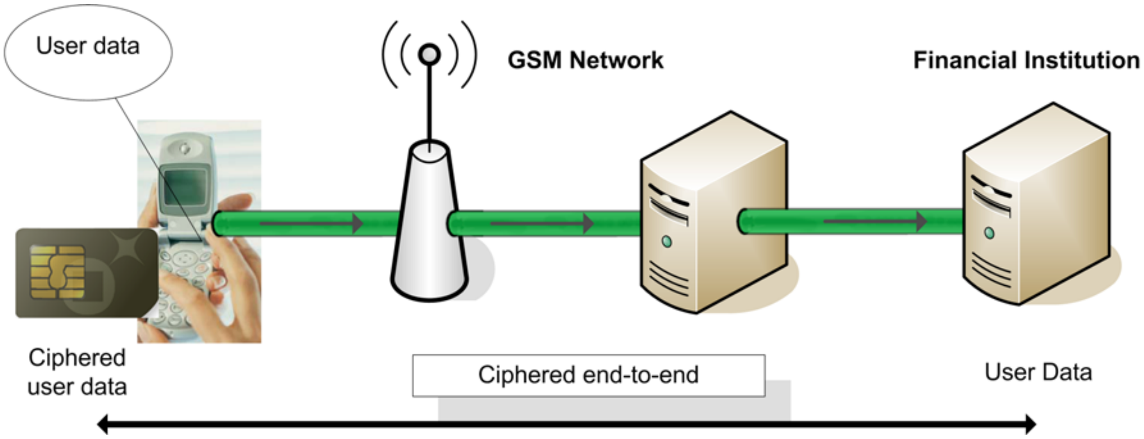
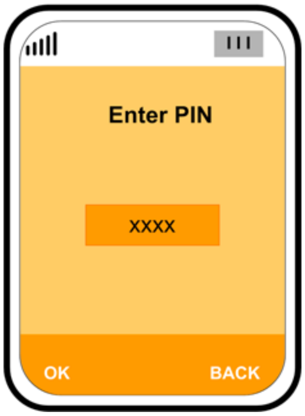


Figure 4: Secure Data Transfer

For the highest level of security, sensitive data, such as PIN and transaction details are never stored in the SIM card 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

Bank customers must be sure that no one can make transactions on their behalf, and banks must be able to verify that customers are indeed who they claim to be. Gemalto responds to this requirement with strong two-factor authentication.



With Mobile Banking:
Users are required to identify themselves to the bank with a Mobile Banking PIN that protects access to financial information and transactions.
Secret keys only known to the SIM card and the bank are used to encrypt and sign transaction data, further proving the identity of the user.

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 to show that the transaction was performed by that party.

Gemalto Mobile Banking 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 (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.

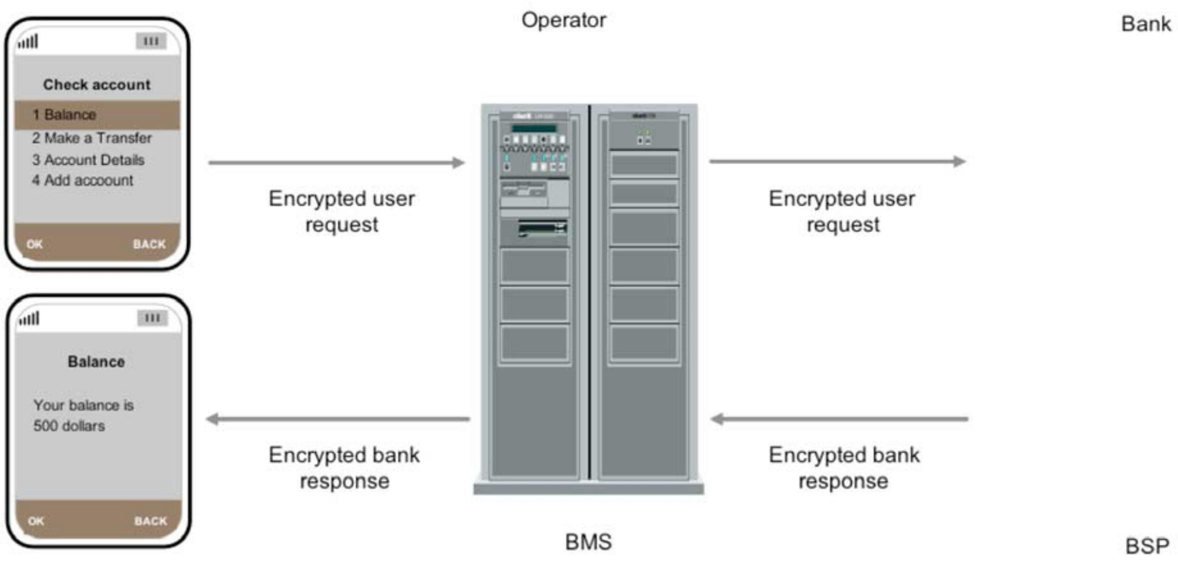
The cryptographic functions, including key management, are performed using the most fraud-resistant hardware solution: a Host Security Module augmented by Gemalto’s firmware, which personalizes the HSM for Mobile Banking. The selected HSM, Thales HSM 8000, is certified as complying to the most stringent security standard: FIPS 140-2 Level 3.

Transaction Flow

A mobile banking transaction is initiated by the mobile user and is completed when the result is displayed on the user's phone. The following example shows the communication flow for an account balance request.

- A customer browses Mobile Banking pages on the mobile phone and requests an account balance from the bank by selecting the account and entering the PIN to confirm the transaction.
- The request is encrypted and signed in the SIM and sent to the BMS via the mobile operator's network through the SMSC and the S@T Gateway.
- The BMS communicates with the BSP at the bank.
- The BSP decrypts information related to the transaction (the account), translates the PIN, translates the request and sends it to the bank system for processing.
- When the BSP obtains the requested information it sends the response back to the BMS.
- The BMS sends the response to the S@T gateway which formats and forwards it to the SIM card in the mobile phone.
- The response is decrypted in the SIM card and presented to the user.
- The mobile user sees the result of her or his request on the phone display.

Figure 5: High-level Communication Flow



Operation and Maintenance

The Mobile Banking platform requires minimal maintenance, mostly consisting of verifying system logs regularly. The maintenance of the platform servers, the RDBMS and the HSM is as specified by the manufacturers of those products.

Mobile Account Management

The standard version of Mobile Banking does not include any mobile account management or billing functionality, since different operators and banks use different account management methods and, often, proprietary billing systems.

Mobile Banking does however allow the operator to configure the BMS with TPDA codes for billable and non-billable SMS messages. Additionally, Gemalto can develop custom mobile account management functionalities tailored to the needs of financial institutions or operators.

Storage of User Information

All the banking records are kept in the financial institution's systems, outside of Mobile Banking. However, the Mobile Banking application needs customer information such as the MSISDN, ICC-ID, client and operator ID required by the BSP to process mobile transactions. This data is stored in a relational database owned by the financial institution. Mobile Banking requires a specific RDBMS, but its administration is left to the financial institution.

Operating System Requirements

The Mobile Banking platform software runs on standard UNIX or Linux servers freeing the operator and the financial institution from the high cost of purchasing and maintaining proprietary operating systems.

Associated Technologies

Mobile Banking uses the following technologies and products:

- Linux or UNIX operating system
- Thales HSM 8000
- Oracle 10g or newer RDBMS
- Standard interfaces (SMS, HTTP, XML, STKML)
- Java, S@T and mini-S@T technologies

Acronyms

3DES	Triple Data Encryption Standard
ATM	Automatic Teller Machine
BMS	Bank Mediation Server
BSP	Banking Service Platform
DUKPT	Derived Unique Key per Transaction
FIPS	Federal Information Processing Standards
GSM	Global System for Mobile Telecommunications
HSM	Host Security Module
HTTP	HyperText Transfer Protocol
ICC-ID	Integrated Circuit(s) Card – Identifier, known as the SIM card Identifier
MAC	Message Authentication Code
MSISDN	Mobile Station International Subscriber Directory Number, known as a phone number
OTA	Over-The-Air
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identity Number
RDBMS	Relational Database Management System
S@T	SIM Alliance Toolbox
SIM card	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Center
STKML	SIM ToolKit Markup Language
XML	Extensible Markup Language

The world leader in digital security

www.gemalto.com

gemalto

security to be free