Tel: (240) 535–2095 ◆ **http://**mobile.setecs.com ◆ **E-mail:** info@setecs.com

SETECS® SAFE™ System

Prerequisites, Products, and Deployment Phases

When the server described in item A.1 is ready, contact SETECS for installation assistance.

1. Introduction and Approach

This document describes various versions of the SAFE™ system, its deployment phases, hardware and software prerequisites for individual phases, and procedures for installation, activation and deployment of the SAFE™ system. Section 2 specifies hardware and software prerequisites that system operator must provide in order to SETECS® Mobile's team to install, configure and activate the system. Section 3 describes all SETECS® Mobile's SAFE™ system components and products. The system should be deployed in four phases described in Section 4 of this document.

The basic version of the system, in Section 4 called Phase 1, should always be installed and activated first. Basic version supports access to the SAFE™ system only using Wi-Fi connection by smart mobile phones, Internet access to the system and various financial transactions based on pre–paid mobile accounts (SAFE™ accounts). This version does not require any external connections of the system to any business partner – telecom provider or a bank. Other types of mobile connections and other mobile services, in Section 4 called Phases 2, 3 and 4, are implemented as extensions of the basic version. They are mutually independent and may be introduced in any time order. Other types of mobile services, like promotion, mobile air–time management, mobile parking payments, mobile bill payments, mobile ticketing payments, location–based services, mobile government subsidies, etc. can also be planed as separate phases of SAFE™ system extensions.

In principle, for the basic version system operator has no additional costs other than core hardware and software prerequisites. In Phase 1 SETECS® Mobile's software products and services are provided free of charge.

For Phases 2, 3 and 4 or for any other system extensions, SETECS® Mobile has internal (customization) and external (additional hardware and software products) costs. Therefore, system operator or customers are expected to reimburse those costs. Their purpose and level depend on the details of the SAFE™ system versions installed in the extension Phases. Specifications are given in Section 4 of this document.

2. Hardware and Software Prerequisites

2.1 SAFE™ Servers

Demo and Limited Deployment Phase: In order to run all SAFE™ Servers, except SAFE™ Card Management System (CMS) Server, hardware requirements are specified in Appendix A.1. In the initial, limited deployment phase, this hardware platform may host SAFE™ Servers 1, 2, 5, 6, and 7 (Section 3). All SAFE™ Servers located on the same hardware platform may handle up to about 50,000 users and about 1,000 transactions per day. SAFE™ Administration Station (item 8 in Section 3) may also be hosted on this hardware platform.

Full Deployment Phase: The system is considered to be in the full deployment phase when it has more than 50,000 registered users and more than 1,000 transactions per day. In this phase the following servers and configuration is needed, shown in Figure 1:

- SAFE™ Web Server should be hosted on a separate hardware platform;
- SAFE™ Communication Server and SAFE™ Payment Server may run on the same hardware platform, probably the one used in the limited deployment phase;
- Database Server should be hosted on a separate hardware platform;
- There should be one separate hardware platform with all components installed: database server, SAFE™ Web Server, SAFE™ Communication Server and SAFE™ Payment Server;
- The complete configuration should be located behind the firewall and VPN Server.

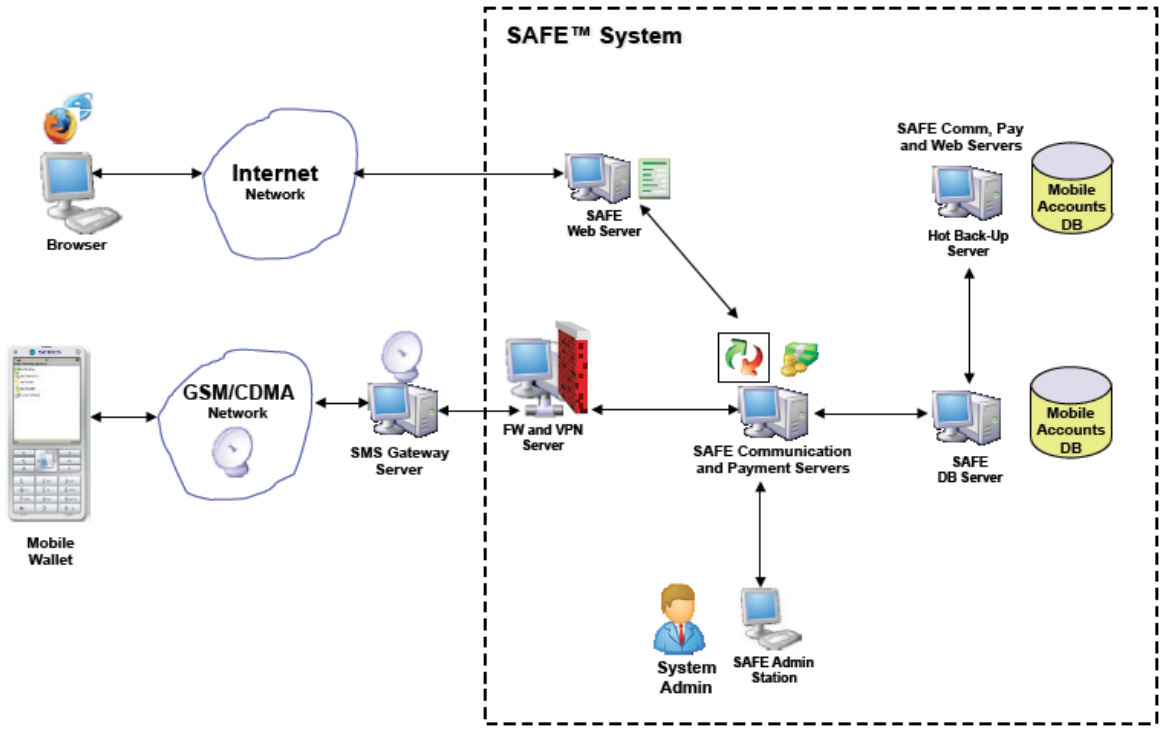

Figure 1: Reliable SAFE™ Architecture and Components

SAFE™ CMS Server (item 4 in Section 3) must be hosted on the separate and equivalent hardware platform. Detailed technical specifications are given in Appendix A.2

2.2 SAFE™ Stations

SAFE™ Administration Station (item 8 in Section 3) is PC with at least 2GB of main memory, reasonable size disk (100 – 200 GB) and Windows XP operating system.

For **SAFE™ CMS Station** (item 3 in Section 3) in addition to the same hardware as for SAFE™ CMS Server, additional accessories are specified in Appendix A2.

2.3 SAFE™ Database

For basic version of the SAFE™ system free version of the MySQL database server can be used. This allows running SAFE™ system in small and medium scaled environments.

For large-scale system, Oracle database server is recommended. We note that this requires separate licenses.

2.4 SAFE Backup Server

Since SAFE™ systems deals with financial data, it is very important to run back-up database server and create continuous database backups and updates. There are different strategies and products available in the market for the database backup. Usually database backup mechanism is the part of all commercially available databases. However, certain vendors, like Oracle, provide additional products for database backup based on users' requirement and criticality of the data. There are two main types of database backups a) **Cold backup**: database is shutdown and all data, logs and control files are backup. b) **Hot backup** is performed while the database is open and available for use. The following products support database backup:

- Oracle 11 g Standard Edition: supports hot and cold backup with remote and incremental backup options. Oracle 11g secure backup module provides policy based and encrypted data backup management.
- MySQL Server Enterprise Edition supports hot and cold backup with remote and incremental backup options.
- SQL Server 2008 Edition supports hot and cold backup with remote and incremental backup options.

SAFE™ hot backup server can use any of the above database servers to backup data based on SAFE™ data backup management policy. We recommend using Oracle 11g Standard Edition as SAFE database.

2.6 VPN Module

The code of different components of the SAFE™ System is totally encrypted. These components are loaded by the specialized SETECS Secure Class Loader. The Loader decrypts different components when loading them in the memory and then executes them. If code is already in JVM, it cannot be tempered or illegally modified. However, in order to protect SAFE™ components from different security attacks, such DOS/DDOS or to prevent against unauthorized access, we are using "secure the perimeter" approach to protect SAFE™ components from different intrusions. We suggest using **secure VPN connection** to protect SAFE™ components and provide confidentiality by blocking intercepts and packet sniffing. VPN also provides sender authentication and hence blocks identity spoofing. There are different professional products that provides VPN and firewall capabilities. Some well-known products are from Cisco, nCircle, Reflex Security, and Symantec. We strongly suggest using **Cisco ASA 5500 Adaptive Security Appliances Series** to implement secure perimeter approach. The above-mentioned product provides strong VPN support. In addition, it allows IPS, anti-virus, anti-spam, anti phishing and URL filtering features. All SAFE™ servers behind SAFE™ Communication Server will be behind Cisco PIX Security appliance, i.e. the Cisco ASA 5500. The said security appliance provides Secure Sockets Layers (SSL) VPN support. SAFE™ system operator should install Cisco PIX 535 Security Appliance for high performance enterprise level security.

2.7 SAFE™ PoS Applications

SAFE™ PoS Application (item 10 in Section 3) is available for the PoS Device produced by New PoS Technologies (www.newpostech.com), model NEW8110. The device must be enabled for Wi-Fi, GPRS and Contactless (RFID) communications.

SAFE™ PoS PC/SCR Application (item 11 in Section 3) currently is under development, so it is not commercially available.

2.8 SAFE™ Wallets

SAFE™ m-Phone Wallet (item 12 in Section 3) is available for Java-enabled mobile phones (Nokia mobile phones with microSD slot), for iPhone and for Android mobile phones. Loading and using this Wallet does not need cooperation with telecom operators that issued mobile phone SIM card.

SAFE™ UICC Wallet (item 13 in Section 3) is available for mobile phones with UICC chip. Loading and using this Wallet needs cooperation with telecom operators that issued mobile phone SIM/UICC card.

SAFE™ SIM Wallet (item 14 in Section 3) is available for mobile phones with SIM chips enabled to host WIB/WML applications. Loading and using this Wallet needs cooperation with telecom operators that issued mobile phone SIM/UICC card.

SAFE™ NFC m-Phone Wallet (item 15 in Section 3) is available for mobile phones with NFC capabilities. Loading and using this Wallet needs cooperation with telecom operators that issued mobile phone with NFC capabilities.

SAFE™ NFC SD Card Wallet (item 16 in Section 3) is available for microSD NFC cards and mobile phones with microSD slot. Loading and using this Wallet needs microSD NFC card provided by SETECS® Mobile and cooperation with telecom operators that issued mobile phone is not needed.

SAFE™ NFC UICC Wallet (item 17 in Section 3) is available for mobile phones with NFC UICC chips provided by SETECS Mobile. Loading and using this Wallet needs cooperation with telecom operators that issued mobile phone with NFC capabilities.

SAFE™ Smart Cards Wallet (item 18 in Section 3) is available for Java smart cards provided by SETECS® Mobile

3. SETECS® Mobile SAFE™ Products

1. **SAFE™ IDMS Server** – The server that performs the following functions:

    1.1 Registration of customers
    1.2 Registration of other SAFE™ Servers
    1.3 Registration of external servers
    1.4 Distribution of registration data to other SAFE™ Servers

2. **SAFE™ PKI/CA Servers** – Certificate Authority (CA) servers organized in a Public–Key Infrastructure (PKI) hierarchy that perform the following functions:

    2.1 Generation of certificates
    2.2 Storage of certificates
    2.3 Distribution of certificates
    2.4 Verification of certificates
    2.5 Generation and distribution of CRLs

3. **SAFE™ Card Management System (CMS) PC Station** – The station that performs the following functions:

    3.1 Registration of SAFE™ customers for issuance of smart cards
    3.2 Enrollment of SAFE™ customers
    3.3 Submission of card issuing requests
    3.4 Activation of SAFE™ smart cards
    3.5 Management and re-issuance of SAFE™ smart cards

4. **SAFE™ Card Management System (CMS) PoS Station** – The station that performs the following functions:

    4.1 Issuing of SAFE™ smart cards
    4.2 Management and re-issuance of SAFE™ smart cards

5. **SAFE™ Card Management System (CMS) Server** – The server that performs the following functions:

    5.1 Storage of card requests and data about issued SAFE™ cards
    5.2 Issuance of SAFE™ smart cards (loading of SAFE™ Wallet and other applets, personalization of SAFE™ smart cards, printing of cards, re–issuance of cards)
    5.3 Over–the–Air (OTA) provisioning of SAFE™ Wallet and other applets

6. **SAFE™ Production Web Server** – Web server that performs the following functions:

    6.1 Registration of SAFE™ customers using Web forms
    6.2 Management of SAFE™ security parameters
    6.3 Management of SAFE™ user profiles
    6.4 Management of SAFE™ mobile accounts
    6.5 Management of SAFE™ transactions

7. **SAFE™ Communication Server** – The server that performs the following functions:

    7.1 Communication with SMS and / or GPRS Gateways of aggregators and/or telecom providers
    7.2 Communication with SAFE™ Payment Server
    7.3 Communication with other SAFE™ Mobile Application Servers (Mobile Ticketing Server, Mobile Bills Server, Mobile Parking Server, Mobile Promotions Server, Mobile Coupons Server, etc.)
    7.4 Communication with other SAFE™ Communication Servers in other domains (system–to–system communications)

8. **SAFE™ Payments Server** – The server that performs the following functions:

    8.1 Communication with SAFE™ Communication Server
    8.2 Communication with EMV Payment Gateway Server
    8.3 Communication with IT processing systems in participating banks and other financial Institutions and financial services providers (remittance, micro–finance, bill payments, etc.)
    8.4 Communication with SAFE™ Production Web Server
    8.5 Communication with other SAFE™ Mobile Application Servers

9. **SAFE™ Administrative Station** – The station that performs the following functions:
    9.1 Administration of the SAFE™ IDMS Server – registration and customization
    9.2 Administration of the SAFE™ Communication Server – communication channels and configuration parameters
    9.3 Administration of SAFE™ Financial Server – registration of banks, accounts, and review of transactions
    9.4 Administration of SAFE™ CMS Station – smart card functions
    9.5 Administration of SAFE™ CMS Server – smart card functions
    9.6 Administration of SAFE™ databases – schema review, backup and hot switching
    9.7 Administration of system logs – review and archiving

10. **SAFE™ System–to–System Server** – The server that performs the following functions:
    10.1 Registration of SAFE™ Payment Servers in individual domains
    10.2 Communication with other SAFE™ Communication Servers in other domains (system–to–system communications)
    10.3 Communication with external Servers of various Financial Services Providers (Remittance Providers, Bill Payments Providers, Currency Conversion Providers, etc.)
    10.4 Receiving and storing system–to–system transaction messages (outgoing messages)
    10.5 Receiving inquiries and sending system–to–system transaction messages (incoming messages)

11. **SAFE™ m-Phone Agent Application** – The application loaded in a mobile phone that supports SAFE™ agent functions:
    11.1 Registration of users
    11.2 Authorization of transactions
    11.3 Request for issuance of SAFE™ smart cards

12. **SAFE™ m-Phone Merchant Application** – The application loaded in a mobile phone that supports SAFE™ merchant functions:
    12.1 Registration of merchants
    12.2 Registration of merchant's location
    12.3 Payment transactions
    12.4 Acceptance of m–tickets, m–coupons, etc.

13. **SAFE™ PoS Merchant Application** – The application loaded in Pont–of–Sale (PoS) devices supporting Over–the–Counter (OTC) payment transactions that performs the following functions:

    13.1 SAFE™ cash–in / cash–out transactions using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards
    13.2 Payments over–the–counter (OTC) using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards
    13.3 EMV transactions – OTC payments or ATM cash–out transactions using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards

14. **SAFE™ PC Merchants Application** – The PC application supporting SAFE™ transactions using desktop Smart Card Reader (SCR), contact or contactless, that performs the following functions:

    14.1 Cash–in / Cash–out using SAFE™ smart cards or SAFE™ NFC Wallet
    14.2 Payments over–the–counter using SAFE™ smart cards or SAFE™ NFC Wallet
    14.3 PIN and fingerprint authentication

15. **SAFE™ m-Phone Wallet** – The application loaded in a mobile phone that performs the following functions:

    15.1 User login using PIN
    15.2 Mobile financial transactions for banked users (m–Banking)
    15.3 Mobile financial transactions for un-banked users (m–Commerce)
    15.4 Merchant–to-distributor, merchant–to–merchant or any business–to–business payments
    15.5 Customer–to–merchant payments over–the–counter

16. **SAFE™ UICC Wallet** – The application loaded in an User Integrated Circuit Chip (UICC) that performs the following functions:

    16.1 Registration of users using mobile phones
    16.2 User login using PIN
    16.3 Mobile financial transactions for banked users (m–Banking)
    16.4 Mobile financial transactions for un-banked users (m–Commerce)
    16.5 Various types of payments transactions (person–to–person, person–to–merchant, business–to–business, etc.)
    16.6 Various security-setting functions

17. **SAFE™ SIM Wallet** – The application loaded in a Subscriber Identity Module (SIM) chip that performs the following functions:

    17.1 Registration of users using mobile phones
    17.2 User login using PIN
    17.3 Mobile financial transactions for banked users (m–Banking)
    17.4 Mobile financial transactions for un-banked users (m–Commerce)
    17.5 Various types of payments transactions (person–to–person, person–to–merchant, business–to–business, etc.)
    17.6 Various security-setting functions

18. **SAFE™ NFC m-Phone Wallet** – The application loaded in a NFC–enabled mobile phone that performs the following functions:

    18.1 Registration of users using mobile phones
    18.2 User login using PIN
    18.3 Mobile financial transactions for banked users (m–Banking)
    18.4 Mobile financial transactions for un-banked users (m–Commerce)
    18.5 Various types of payments transactions (person–to–person, person–to–merchant, business–to–business, etc.)
    18.6 Merchant–to-distributor NFC payments (OTC)
    18.7 Customer–to–merchant NFC payments (OTC)

19. **SAFE™ NFC SD Card Wallet** – The application loaded in a NFC–enabled microSD card that performs the following functions:

    19.1 Registration of users using mobile phones

19.2 User login using PIN
19.3 Mobile financial transactions for banked users (m–Banking)
19.4 Mobile financial transactions for un-banked users (m–Commerce)
19.5 Various types of payments transactions (person–to–person, person–to–merchant, business–to–business, etc.)
19.6 Merchant–to-distributor NFC payments (OTC)
19.7 Customer–to–merchant NFC payments (OTC)

20. **SAFE™ NFC UICC Wallet** – The application loaded in a NFC–enabled User Integrated Circuit Chip (UICC) that performs the following functions:

20.1 Registration of users using mobile phones
20.2 User login using PIN
20.3 Mobile financial transactions for banked users (m–Banking)
20.4 Mobile financial transactions for un-banked users (m–Commerce)
20.5 Various types of payments transactions (person–to–person, person–to–merchant, business–to–business, etc.)
20.6 Merchant–to-distributor NFC payments (OTC)
20.7 Customer–to–merchant NFC payments (OTC)

21. **SAFE™ Web Payment Module** – The module combined with Web cash–out pages that enables SAFE™ customers to pay Web purchases using SAFE™ mobile accounts

4. Deployment Phases

4.1. Summary of the Approach

This section describes the proposal by SETECS® Mobile Technologies ("SETECS® Mobile") to system operator for installation, activation and deployment of the SAFE™ system. The proposal is based on SAFE System Description document. The system will be established in four phases, all four together will last approximately six months. In each phase there will be deliverables and operational mobile services, so that system operator will be able to commercially deploy the system already after completion of the first phase. Basic version of the SAFE™ system is treated as Phase 1 of the project. The version of the SAFE™ system installed in Phase 1 uses only SMS messages and supports various mobile financial transactions based on pre–paid SAFE™ mobile accounts.

Deliverables and new mobile services in subsequent phases (Phase 2 – 4) are introduced as extensions of operational mobile services activated in Phase 1. At the end of the proposed six months extensions and setup activities, all subsystems of the SAFE™ system will be fully integrated, operational and in production, so the system will be ready for large scaling, for introduction of new mobile services, and for extensions with new customers (companies) and users (subscribers).

After the system is activated in Phase 1, subsequent Phases, their deliverables and new services are mutually independent of each other. So they can be introduced in any order or even in parallel. Mobile Promotions subsystem, as extension of the system introduced in Phase 1, can also be planned as an extension. It will require planning and scheduling equivalent to the extensions proposed in this document.

4.2. Phase 1: Mobile Financial Transactions using SMS Messages and Mobile Accounts

Mobile Services: At the end of this phase the following **mobile services** will be operational, all based on use of **mobile pre–paid accounts** and use of **SMS messages**:

- Registration of system officers, system agents, users and merchants using mobile phones
- Opening and use of pre–paid mobile accounts (unbanked users or users with bank accounts, but using only mobile pre–paid accounts)
- Cash–in and cash–out operations with mobile accounts using agents ("Mobile ATM")
- Payments to merchants over the counter using mobile phones
- Person–to–person transfers using mobile phones
- Account status inquiries

Deliverables / Components: SETECS® Mobile will deliver one copy of each of the following software components of the SAFE™ system:

- SAFE™ Communication Server

- SAFE™ Payments Server
- SAFE™ Web Server, and
- SAFE™ Administrative Station

SETECS® Mobile will also deliver technical, marketing, end educational documentation for the system. Technical documentation includes Administration and User Manuals. Marketing documentation includes User Leaflet. Educational documentation includes Technical White Paper, Business White Paper, and Operational PPT.

Services: In this phase SETECS® Mobile team will provide local technical assistance services: install *SAFE™ Communication Server, SAFE™ Payments Server, SAFE™ Web Server*, and *SAFE™ Administrative Station*. SAFE™ Web Server will be *customized* by Web designer/developer to reflect joint, system operator and SETECS® Mobile, operations. SETECS® Mobile will also provide technical assistance for linking the system to the *telecom aggregator* and it will use only SMS messages. SETECS® Mobile will provide telecommunication services to system operator. Subscribers of all telecom operators in South Africa will be able to access and use the system. SETECS® Mobile will also provide *education* and *training* to system operator's personnel. In this phase, SETECS® Mobile will also provide *system administration* services to system operator.

Prerequisites: system operator will be responsible for technical, organizational and financial prerequisites. Technical prerequisites are Win 2008 Server and open Internet connection. In addition, system operator will provide hosting environment: uninterrupted power supply, network protection components (like firewall and VPN), and technical assistance for installing, customizing, activating and operating the System. Organizational prerequisites are all activities necessary to register and activate the planned number of agents, including their education, organization, and financial arrangements.

Duration / Schedule: This phase will last **one month**. It will be scheduled within Month 1 of the project.

4.3. Phase 2: Mobile Financial Transactions using Bank Accounts

Mobile Services: In this phase the following new mobile services will be introduced, in addition mobile pre–paid accounts and SMS messages from Phase 1, these services will use **software components** loaded in **mobile phones** and **PoS devices** and **GPRS messages** (if 3G is available in South Africa):
:

- Registration of bank officers using mobile phones
- Opening and use of bank accounts (users with bank accounts)
- Cash–in and cash–out operations with bank accounts using agents or bank branch offices
- Payments to merchants over–the–counter (OTC) using mobile phones and PoS devices
- Account–to–account bank transfers using mobile phones
- Account status inquiries

Deliverables / Components: SETECS® Mobile will deliver the following software components of the SAFE™ system:

- SAFE™ Mobile Banking Module
- SAFE™ Trusted Services Management (TSM) Server
- SAFE™ SIM Chip Wallet (loaded in SIM chips for regular phones)
- SAFE™ Java Midlet Wallet (mobile application for smart and high–end phones)
- SAFE™ NFC Wallet (loaded in NFC microSD cards or NFC SIM chips)
- SAFE™ PoS Station and Application
- SAFE™ Web Payment Module for Web merchants using mobile and bank accounts

SETECS® Mobile will also deliver technical, marketing, end educational documentation for the new components of the system.

Services: In this phase SETECS® Mobile team will first customize its SAFE™ Mobile Banking Module to exchange financial messages with IT Servers of the participating banks. Four banks are planned to participate in this project. SETECS® Mobile will also cooperate with participating telecoms in order to establish, test and activate over–the-air (OTA) provisioning system for the SIM Wallet. SETECS® Mobile will assist system operator team to distribute, connect and activate SAFE™ PoS devices with participating merchants. Ten merchants are planned to participate in this pilot. In this phase 10 Web merchants will be enabled to accept mobile payments from their Web Servers.

Prerequisites: Active cooperation and support of the cooperating banks, merchants and telecom operators is needed. Banks will provide assistance with testing of connections between SAFE™ Mobile Banking Module and Bank IT systems. Telecoms will provide assistance with loading SAFE™ SIM or NFC Wallets using SAFE™ TSM Server.

Duration / Schedule: This phase will last **two months**. It will be scheduled within Month 2 and 3 of the project.

4.4. Phase 3: Mobile Financial Transactions using SAFE™ Smart Cards

Mobile Services: In this phase the same financial services as in the previous two phases will be available, only extended with use of the SAFE™ smart cards. If system operator also want to use SAFE™ Combo Cards, supporting VISA/MasterCard bank card transactions using magnetic stripe or EMV–compliant chip, SAFE™ smart cards will be extended to support also bankcard transactions.

The following services will be available to manage SAFE™ smart cards, integrated with existing bankcard management procedures used by participating banks:

- Registration of cardholders and creation of card issuing requests
- Enrollment of cardholders (capturing of biometric and facial data)
- Issuing cards (printing and electronic personalization of chips)
- Distribution, activation and administration of smart cards
- Managing (requesting, issuing and distributing) X.509 certificates

The following financial services will be available using SAFE™ smart cards:

- Cash–in and cash–out operations using PoS devices with merchants
- Payments to merchants over–the–counter (OTC) using PoS devices and smart cards
- Account status inquiries using PoS devices and smart cards

Deliverables / Components: SETECS® Mobile will deliver the following software components of the SAFE™ system:

- SAFE™ Smart Card Management Server
- SAFE™ Smart Card Management Stations
- SAFE™ Smart Cards
- SAFE™ Smart Card Wallet Applet / NFC Wallet Applet
- EMV Wallet Applet (Optional)
- SETECS® OneMAN™ IDMS Server
- SETECS® OnePKI™ CA Server
- SETECS® OnePKI™ Certificates

SETECS® Mobile will also deliver technical, marketing, end educational documentation for the new components of the system.

Services: In this phase SETECS® Mobile team will install and activate SAFE™ Smart Cards Server that will receive request and issue SAFE™ Smart Cards. It will also install two SAFE™ Smart Cards Stations with two smart card readers and a camera for enrollment of users. In this project, SETECS® Mobile will also be in charge of all SAFE™ smart card management operations. One thousand cards are planned to be issued in this project, loaded with both – SAFE™ Wallet applet and EMV applet.

Prerequisites: Three PCs as hardware components for SAFE™ Smart Card system.

Duration / Schedule: This phase will last **two months**. It will be scheduled within Month 4 and 5 of the project.

4.5. Phase 4: Mobile Commerce (Business–2–Business Mobile Transactions)

Mobile Services: In this phase the following new mobile services will be introduced for business–to–business (B2B) mobile transactions:

- Registration of business entities
- Loading bills and invoices into the SAFE™ system
- Mobile notifications and warnings for bill/invoices payments
- Payments of bills and invoices by individuals and/or business entities

- Bill/invoices payments and account status inquiries

Deliverables / Components: SETECS® Mobile will deliver the following software components of the SAFE™ system:
- SAFE™ Invoices Server (B2B mobile transactions)
- SAFE™ Bill Payments Server (B2P mobile transactions)

SETECS® Mobile will also deliver technical, marketing, end educational documentation for the new components of the system.

Services: In this phase SETECS® Mobile team will install and activate SAFE™ Invoices Server, which will provide on–line connection between SAFE™ system and Accounting Servers of the participating business entities, and SAFE™ Bill Payment Server, which will distribute utility bills and individuals. SETECS® Mobile will also link two servers with SAFE™ Payments Server, so that bills and invoices will be paid using mobile accounts. One utility company is planned in this project.

Prerequisites: Active cooperation of bill–issuing companies is needed

Duration / Schedule: This phase will last two months. It will be scheduled within Month 5 and 6 of the project.

Appendix: Detailed Technical Specifications

A.1 Specifications for SAFE™ Servers

For all SAFE™ servers except SAFE™ CMS Station and Server, the following are hardware requirements:

- Quad-Core 64-bit CPU with 2.8 GHz or higher
- 8 GB of main memory
- 400 GB of disk space (possibly RAID 1)
- 100 Mbit network adapter
- One public IP address with Internet access
- Windows Server 2008, 64-bit
- One user registered (user name and password)
- Windows Remote Connection enabled

A.2 Specifications for SAFE™ CMS Components (Station and Server)

1. Workstations..... Qty. 2

- Operating system: Windows XP Professional
- Processor: min. 2.2 GHz, 4 MB cache, 800 MHz memory
- Memory: min. 16GB DDR2 800 MHz
- Hard drive 160 GB 7200 rpm SAT
- Optical Drives: DVD+RW
- I/O Ports: min. 6 USB 2.0: PS/2; 1 RJ-45 to integrated Gigabit LAN; 1 serial;
- Graphics and Input/Output devices: NVIDIA Quadro 256MB PCIe
- Monitor: LCD HD 17", resolutions to 1280 x 1024,
- USB standard keyboard
- USB optical scroll mouse

2. Smart Card Printer..... Qty. 1

- Fargo HDP 5000, Part #: 89035
  Base Model, 16MB Memory, 110-240 VAC,
  Double Side High Definition Printing
  Smart Card Encoder, HID Prox and Contact Smart Card Encoder
  (Omnikey Cardman 5125*)

- YMCKK Cartridge (Part#: 84052)
  Full-color ribbon with two resin black panels

- HDP Film Cartridge (Part#: 84053)
  Approximately 1,500 images

3. Desktop Smart Card Readers..... Qty. 3

- USB Smart Card Reader
- Type: (301087) SCR3311 (904613 USB Smart Card Reader)
- Manufacturer: ST Microsystems
- Deliverer: Envoy Data Corporation

4. Fingerprint Smart Card Reader..... Qty. 2

- Type: Precise Model 250MC
- Manufacturer: Precise Biometrics

5. Canon PowerShot Camera ..... Qty. 2

10 Megapixel Digital Camera with 4x Optical Zoom including tripod, case and cleaning kit supporting remote shooting. The PowerShot models listed below are known to support Remote Shooting on Windows XP:

Pro series: Pro90IS, Pro1
G-series: G1, G2, G3, G5, G6, G7, G9, G10

S-series: S30, S40, S45, S50, S60, S70, S80, S1 IS, S2 IS, S3 IS, S5 IS, SX100 IS, SX110 IS
A-series: A30, A40, A60, A70, A75, A80, A85, A95, A300, A310, A400, A510, A520, A620, A640
Digital IXUS: SD100 (Digital IXUS II), SD110 (Digital IXUS IIs), S230 (Digital IXUS 330), S400 (Digital IXUS 400), S410 (Digital IXUS 430), S500 (Digital IXUS 500)

6. Radio Shack AC adapter for Canon Camera ..... Qty. 2
- 3 V ,1000A
- Cat. No. 273-1680 A