

SETECS® Mobile Technologies
USA

SAFE™

Security System
for Mobile Transactions
and Applications



www.setecsmobile.com

Reliable Registration of Users

- Face-to-face validation of user identity (Know-Your-Customer)
- Confirmation of registration and PIN by user



Authentication of Users

- Wallet PIN
- SAFE™ System PIN

Wallet Data Protection

- Confidentiality of Wallet data using encryption
- Integrity of Wallet data using hashing



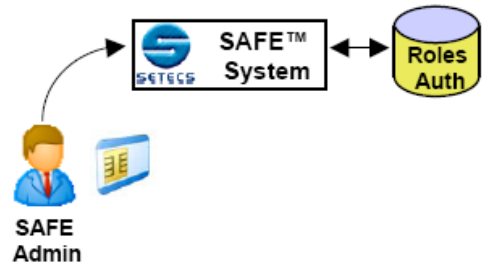
Message Security

- Confidentiality of data in messages using encryption
- Integrity of data in messages using hashing



Authorization

- SAFE™ system roles: system administrators, system officers, agents, and users)
- Authorizations of transactions
- Login by system administrators using smart cards



Security of Transactions

- Verification of the initiator
- Confirmations of transactions by agents
- Financial policy with rules and restrictions



SIM / UICC Chip Cryptography

- DES cryptographic algorithm
- 3DES strong cryptographic algorithm
- AES cryptographic algorithm
- RSA digital signing and digital enveloping algorithm
- Secure channel with the SIM / UICCC chip



SAFE™ Smart Cards

- Protection of data stored in smart card chip
- Authorization of transactions using PIN
- Biometric fingerprint authentication
- Encrypted stored money and card credentials
- Photo stored in the card (FIPS 201)
- Authentication certificate stored in the card (FIPS 201)



SAFE™ System Security

- Protection by firewall
- Protection of communication messages by Secure Socket Layer (SSL) protocol between components
- Secure connection with external components (Secure Web Services)
- On-line hot backup of data
- Encryption of all system software modules which are resistant to viruses, worms and hackers

