RTS Risk Management Guide

TABLE OF CONTENTS

Introduction

This document describes the Risk Management System of the Remote Transaction System (RTS) Solution. The guide describes the combination of technical and operational mechanisms that have been put in place across the RTS value chain to mitigate security breaches that could result in a loss for any of the parties in the value chain – clients, agents, or the microfinance institution. The guide assumes that the financial institution in question is using independent third-parties, such as merchants, as the agents.

The risk management approach described in this guide is primarily intended for the executive management team of the financial institution and for regulatory bodies, such as the national bank. The purpose of this document is to demonstrate that the risks to microfinance institutions introduced by the RTS Solution can be effectively mitigated and monitored.

Elements of Risk

Risk Management refers to a system that allows an institution to identify, measure, and manage the business risks it faces. The RTS solution will impact a financial institution through financial and operational risk. Financial risks include credit risk, liquidity risk, interest rate risk and foreign exchange risk. The RTS should have a net positive impact on financial risk. Operating risks include fraud and transaction risk. Strategic risks include governance, business and external risk. Technology and operational features that need to be developed to mitigate increased operational risk as a result of the introduction of the RTS are described in this document.

Financial Risk

The RTS solution should have a net positive impact on a financial institution's ability to manage its financial risk in several ways. First, by providing more accurate, timely and electronically based information to the institution, the solution should help lower the institution's financial risk. Increased access to higher quality information will reduce the credit, liquidity and interest rate risks of a financial institution, by allowing the institution to make better decisions in a more adequate time frame. In addition, the RTS solution will provide a mechanism for more simplified and transparent operations, and more direct accountability to clients.

Operational simplicity and transparency are achieved through the point-of-sale (PoS) devices' ability to automatically generate off-setting accounting transactions on the accounts of the clients and the PoS operator, or agent. The business rules for all allowed PoS transactions (there are currently four: loan payment in cash; loan payment via transfer from savings account, savings deposits, savings withdrawals) are stored on the PoS and applied to the clients and PoS agents' accounts as part of the transaction.

More direct accountability to clients is achieved by improving on the level of access that clients have to their account information. Clients maintain a record of their ten last transactions on their smartcard, along with balances on their savings accounts and loan accounts, and are provided machine printed receipts (with unique serial numbers) for all transactions.

Operational Risk

In any financial institution, there are also a number of operational risks, such as transaction and fraud risk. The introduction of the RTS within UMU's business will expose the microfinance institution to two forms of operational risk.

- Transaction risk - financial loss resulting from system error, human error, negligence, or mismanagement

- Fraud risk – loss to earnings or capital due to intentional deception by employees, clients or agents

These risks will be easier to track with the RTS because the system provides faster tracking and reporting on both loans and the flow of funds. In any lending environment, enhanced monitoring always improves the risk profile by allowing management to react to negative situations rapidly. The RTS also limits risk as a result of the redundancy elements that have been built into the system. This level of duplication does not exist in the old paper-based system

Even though some elements of operational risk can be mitigated by the RTS, other types of risk are introduced as a result of the system. These challenges include intermittent GSM network connectivity, asynchronous data management resulting from dual-mode capability, multiple party involvement and a potentially state-disconnected system distributed across several rural geographic locations. The potential for data to become outdated, lost or overwritten due to inappropriate update procedures and the high potential for fraud through transactions that occur outside of the RTS system – especially by third-party agents – pose significant challenges.

This document seeks to address the security features of smart card solutions, describe industry standards and best practices, and recommend appropriate security enhancements and process flows that minimize the costs and risks of the RTS solution.

Risk Management

The primary pillars of data security are prevention, detection and remediation. The security of every link in the security chain must be reviewed to adequately design adequate methods to detect, measure and isolate fraudulent activity[1] and finally, establish countermeasures for appropriate responses to security breaches. [2]

Prevention

Prevention is the most critical element for obvious reasons. The majority of the financial decisions, technology implementations, and business practices described in this document have been implemented with the intention of preventing any form of fraud.

The most important elements of fraud prevention have been built in the technical components of the RTS solution. The smart cards, PoS terminal, transmission software, and back-end systems have all been developed to perform critical preventive functions, such as data encryption, authentication, and authorization.

> **Encryption** is a means of scrambling information so that data remains confidential. Different forms of this technique are being used on the smart cards, in the PoS terminals, and within the data packets that are transmitted across the cellular network and through the servers.
>
> **Authentication** verifies that the parties, such as clients and agents, are who they claim to be. Authentication should still be performed by the financial institution through its client screening procedures, which should not change in this system. Authentication is also performed through biometric data on the smart card, and within the technology itself.
>
> **Authorization** confirms and restricts what an authenticated party can do within the system. This includes restricting access to transacting data, limiting the amount of money that can be withdrawn in any given day, and enabling the financial institution to withdraw privileges from an agent or client when deemed necessary.

In addition to the security features deployed in the technology, the institution's operational procedures will play a critical role in fraud prevention. The financial institution should establish levels of accountability for its staff, clients, and agents. Some elements of accountability will be set within the technology and others need to be integrated into the institution's ongoing operational procedures and business practices.

[1] Everett, Dr. David B., "Smart Card Tutorials 2", Smart Card News, 1996.
[2] Smart Card Alliance website: www.smartcardalliance.org

Detection

Detection refers to a series of procedures that can be used to alert the financial institution of potential fraud, ensuring that problems are dealt with quickly. For large electronic payment systems, such as VISA, very sophisticated fraud detection software and analysis tools are in use. One detection company has accumulated a database of over 200 million transactions that it uses to ferret out fraudulent activity. Unfortunately these tools are far out of the reach of many microfinance and other smaller financial institutions. Until enough transaction volume has been generated to justify the development of software tools, the majority of detection procedures should be carried out manually by internal accounting staff.

Remediation

Remediation is the set of activities taken after a security breach has occurred to resolve the immediate problem and adjust procedures to eliminate the possibility of repeated infringements.

As described by a senior risk management team, it is never commercially viable to build a completely secure system. We will always have to judge the best mix of technical security and operational security. And we also have to recognize that security is an iterative process.

Assessing and managing risk within an institution is an ongoing process. As RTS is implemented, it will be imperative that the financial institution continue to identify potential risks the solution presents, develop strategies to measure and mitigate those risks, and implement new controls. As the rollout continues, a full internal audit will/should be conducted to identify potential weaknesses.

Transaction Process Flow

For security purposes, each agent card is linked to only one PoS terminal. Clients should be limited to the amount of funds they can withdraw in a day.[3] Agents should be limited by the amount of money they can accept each day. Both agents and clients should have a minimum savings account balance as well.

At the end of each day, agents should go through a close-of-day process that will produce a summary report of their transactions and automatically upload the transactions on the PoS. This link will also download any text messages that have been sent by the financial institution to the agents.

When a client arrives at the agent with an initialized smart card, they proceed through the following steps:

- The agent inserts her smart card into the PoS, and provides a pin number. This process authenticates the card holder as the agent assigned to this device
- The client inserts her card into the terminal and inserts her pin number
- One of five transaction types is requested by the client:
  - Loan repayment
  - Savings deposit
  - Savings withdrawal
  - Fund transfer
  - Balance lookup
- The amount of payment is entered
- A screen appears summarizing the transaction
- Upon acceptance of the summary screen, the balance on client's card is updated. A client card will hold a transaction history of up to 10 transactions. Prior to updating, any transaction fees will be deducted to ensure that the account balances on the client and agent cards match the back-end.
- The agent reinserts her card so the balance on her card can be updated and the transaction stored. An agent card will hold up to 300 transactions.
- The PoS terminal prints two receipts, one for the client and another for the agent.
- The client will sign the agent receipt.

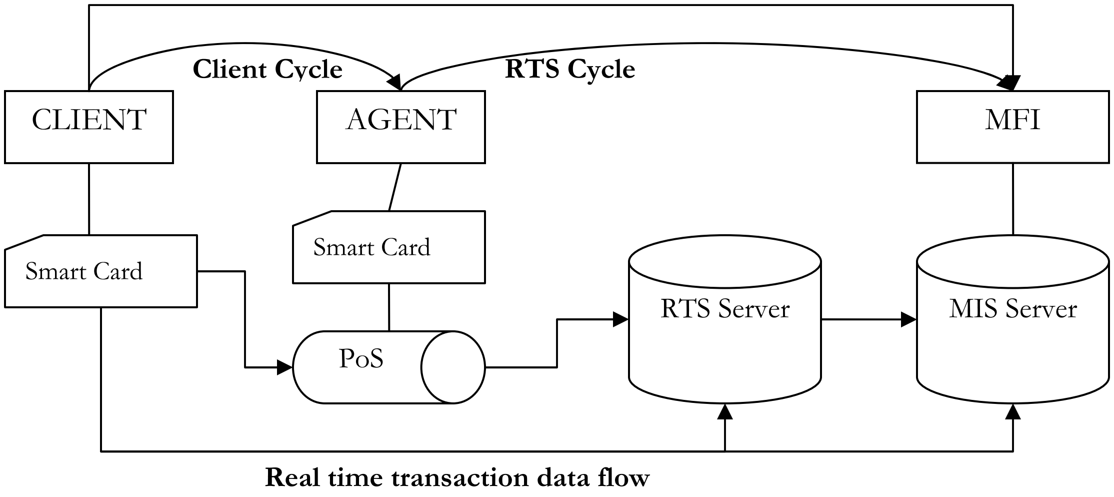
The PoS device operates in two modes – online and offline. In the online mode, back-end accounting systems are accessed during the transaction. No transactions are saved to the PoS device. In the offline mode, the transaction is saved on the client card, the agent card, and the PoS device. At the end of the day, the transactions are uploaded from the PoS device to the back-end systems. When successful, these transactions are removed from the PoS device. The agent card can hold up to 300 transactions and it can serve as a secondary storage in case of a PoS failure.

[3] The financial institution sets the start time of each day, which is defined as a 24-hour period. The institution also determines the parameters of a weekend.

RTS Risk Management System

RTS Value Chain

In the course of an RTS transaction and the subsequent upload of the transaction data to the RTS server and the financial institution's back-end systems, there is a value chain that includes the smart cards, clients, agents, PoS terminal, data transmission, RTS server, and MIS server.



Each of the links in this value chain presents unique security risks, and each of the links needs to be managed individually through the risk management system to minimize that risk. The greatest points of risk along the chain are those places in which money changes hands. Threats to the security of data can be internal (staff) or external (hackers, rogue viruses, interceptions, etc.). External attacks tend to focus on weaknesses in the transmission of data and find points of interception – this often starts with the card.

Smart Card

Card Design

Smart cards are commonplace globally and are becoming critical for security in online financial applications. Smart cards are microprocessor or memory cards that rely upon a program interaction between the PoS device and the smart card.

The on-board microprocessor and data capacity embedded in smart cards can provide secure, offline processing. The financial industry has attempted to mitigate the risk of external attacks by deploying smart cards to encrypt and store user and account information. Those cards employed with Public Key Encryption (PKI), keys ensure a high level of security because they utilize every mechanism of data security available in an embedded and coordinated manner.[4] Europay, MasterCard and Visa (EMV) have set the standard for financial institutions employing smart card technology worldwide. The global EMV specification allows smart cards to support chip-based credit and debit transactions, similar to how magnetic stripe cards are used today.

There is a worldwide migration to the EMV standard underway which is premised upon the belief that chip-based cards will offer greater security and lower fraud than magnetic strip cards. Banks in Europe were required to be EMV-ready by January 2005. Those that were not ready were assigned the liability and assume the costs associated with fraudulent transactions. Visa International's EU region expects 75% of cards and 90% of terminals to be EMV-ready by January 2005. Banks in Asia-Pacific face a deadline the following year, and other regions, except for North America, face mandates, too. [5]

RTS System

- AT88SC1616C 2K byte cryptomemory cards, which have memory chips[6]
- EMV L1 compliant. Highest level of standard is now 4.3. RTS cards do not take advantage of all EMV security features, many of which are intended for more sophisticated markets.

Data Encryption

Another important security feature of smart card technology is that it includes a renewable security element. In other words, cryptographic keys and algorithms can be changed if the system is compromised.

RTS System

- Data on the smart cards is encrypted via the standard PKI format.
- There are two keys, a public key and a private key. The public key, on the PoS, encrypts the data. Then the private key, on the RTS server, decrypts the information. Sharing of the encryption key compromises security. Therefore, only the RTS development team will ever have knowledge of the private key.

Card Authentication and Authorization

A series of steps in the security process determine if the agent and clients' smart cards are authenticated and authorized by the system. These steps verify the identity of the

[4] Smart Card Basics website

[5] Balaban, Dan, "Getting a Grip on EMV", CardTechnology.com website

[6] Originally we had planned to use programmable microprocessor cards, which have a higher level of data management security. However, they are much more expensive – basically a 1:7 difference in price. As a result, many of the security features of EMV are not part of the RTS. For this environment, operational safeguards are more effectively and less costly.

cardholder and determine whether they are authorized to perform the requested transaction.

U.S-based financial systems operate in a real-time environment, with the access point confirmed client account information before a transaction can proceed. Since telecommunication costs are higher in Europe than in the U.S., European issuers have realized telecommunications savings by allowing transactions in an offline mode.[7] This approach reduces their costs dramatically and increases reliability. .

Offline poses more of a risk than online transactions and more safeguards need to be put in place to enable this type of system. Authentication and authorization occur during the communication between the smart card and the PoS terminal. Use of personal identification numbers (PINs) and biometric data at the point of sale lowers risk.

RTS System

- Each smart card has a unique card id that is locked onto the card during manufacture.[8]
- Through a programming step, the unique card id is linked to a specific agent or client. The programming takes place through a special PoS terminal that can only be managed by authorized personal. The terminal is password protected.
- In an online mode, the client card is authorized by the RTS server. When transactions occur offline, risk is mitigated though the pin and a set of procedures that notify Agents of delinquent cards. At end of day uploads, fraudulent cards can also be detected, but risk should be minimal because of transaction limits.
- Since agent cards are linked to a specific PoS terminal, authentication of the agent occurs at the PoS in both online and offline modes.

Client

Client Authentication and Authorization

The point at which funds change hands represents one of the weakest links from a security perspective. It is very important to prove the identify of the agent and client, confirm that they can not go outside limits that have been set for them by the financial institution, and set up procedures that mitigate risk in cases of attempted fraud.

RTS System

- Clients should be approved by the financial institution according to that institution's current client acceptance practices. Approved clients should sign an agreement concerning the use of the card and their responsibilities.

[7] Furletti, Mark, "An Overview of Smart Card Technology and Markets", *Discussion Paper: Payment Card Center, April 2002*, Federal Reserve Bank of Philadelphia, pp. 7.

[8] This is actually a very long time stamp, down to the millisecond, so the probability of two cards having exactly the same ID is very low. In addition, it would be very difficult for anyone to fraudulently create or repeat such a time accurate ID.

- Once approved, clients are given a smart card that only they have been authorized to use. They are also given a unique pin number and taught about the security features of that pin. Education and awareness with clients is a key to successful implementation. Adding photographs to the cards should be considered as client volume increases. Fingerprint authentication is much more secure, and more expensive, approach.
- When the client goes to the agent, they must produce their card and their pin number
  - If the risk analysis recommends it, and the cost is not prohibitive, financial institutions can consider adding photos or fingerprint authentication to the card as an additional form of identification
- A unique receipt is produced at the conclusion of each transaction.
- Client signs agent receipt.

Offline Transactions

Banks in several countries, including France, Germany, the United Kingdom and Italy, have opted for offline transactions as a default mode with certain conditions defining the requirements for online transactions. French banks go online for approval with their domestic chip card only 15% to 20% of the time. One extra precaution they take is to customize the risk parameters for each card—by changing the threshold at which a card will instruct a terminal to call the issuing bank for approval. With EMV, banks can more easily send and store individual commands to cards already in the field.

Issuers have already begun rewarding their good credit risks with a high percentage of offline transactions with certain exceptions that instruct the cards to go online in specific instances, which translates into shorter transaction processing time. For those clients who pose a greater credit risk, online transactions can be customized to the card to require more frequent online authorization.[9]

RTS System

- The financial institution should set limits for their clients and agents
- The financial institution should also set procedures for transacting at the branch
- If a client card is reported lost or stolen, the institution can broadcast the fraudulent card numbers to their agents who will have a responsibility to track the cards. Cards that have not been used will after a preset period will "time out."

Agent

Agent Authentication and Authorization

In the field, the greatest form of accountability is the bonding of the agents. Financial institutions will be responsible for selecting their agents and, thus, for the integrity of their agent network.

[9] Balaban, Dan, "Getting a Grip on EMV", CardTechnology.com website

RTS System

- All agents should be clients of the financial institution until the RTS is capable of switching transactions between financial back-ends.
- Once approved, agents are given a smart card that only they have been authorized to use. They are also given a pin number and taught about the security features of that pin. In addition, the agent will be linked to one, and only one, PoS device.
- Agents should sign an agreement with their financial institution that describes their agreement.
- Agents should be required to sign the client's receipt as further acknowledgement of the transaction and the acceptance of funds

Offline Transactions

To provide safeguards against fraud the amount of transactions that an agent can perform should also be set by the financial institution then monitored by the RTS system.

RTS System

- Limits should be set on the amount of money that each agent can accept in a day
- Each transaction will result in fund balances being transferred from the client's card balance to the agent card balance. Thus each transaction results in a debit to one card, and a credit to another card. This replication of data makes it much harder for an agent to fraudulently claim that they have not received funds. This same data will also be captured by the PoS device.
- Each transaction is captured in seven places, the client card, the agent card, the receipts, the PoS terminal, the RTS server, and the MIS.
- Agent cards will store up to 300 transactions, thus serving as a data master
- At the end of each day, all agents must upload the transactions on their PoS device to the RTS server. If there are pending transactions still on the PoS device the next day, the agent will not be able to transact again until they have uploaded all pending transactions.
- As the volume of transactions increase, agents may need to upload their PoS devices more frequently.

PoS Terminal

The PoS device is a very critical element of the value chain because it is here that the software and rules that control the smart cards reside.

Agent Authentication

RTS System

- Before an agent is given their PoS terminal, their smart card is "locked" to that terminal. This is accomplished through a direct connection between the PoS

terminal, the agent card, and the RTS server. It can only be carried out by authorized RTS technical support staff.
- Once the PoS device is locked to an agent, each time the agent attempts an offline or online transaction the PoS device will confirm the identity of the agent, the identity of the PoS terminal, and the match between the two. If there is any discrepancy, the transaction can not proceed. If a different agent tries to use the PoS, the device is locked. RTS technical support must be called to reinitialize the device.

PoS to RTS Authentication

RTS System

- PoS terminals are initialized by loading a unique PoS program onto the PoS terminal. The program, once loaded, can only be run on that particular terminal. Attempting to load the same program on another terminal will cause errors at the RTS server during transactions.
- Each PoS terminal has a unique name. This name is the publicly available form of the device id number which is hard-coded into the chip of the PoS terminal.
- Transaction packets submitted by each PoS terminal to the RTS server contain information about the PoS device name and device id. This is a form of PoS authentication because only one device can send the correct device id number to the RTS server.
- The PoS software also contains a port number, which means that it can only connect and send data to one RTS server.

Data Transmission

Data is transmitted from the PoS terminal to the RTS server in one of two ways, either across a serial cable that directly links the PoS device to the RTS server or through the GSM infrastructure.

Serial Cable

The encryption of data transmitted between the PoS device and the RTS server via a serial cable would require a great deal of computing power and battery life. Rather than incur such a cost, transmission of data across the serial cable will be restricted to authorized RTS and the institution’s personnel.

GSM Infrastructure

RTS System

- When an agent uploads information from the PoS terminal, each transaction is sent as a separate packet. The data that is transmitted has been encoded and compressed. There are actually two levels of compression in the process. This adds further security features and also ensures that the data is in the smallest possible form when it is transmitted, reducing connection costs and potential errors.

- Each data packet is encrypted using industry standard SSL 128-bit (secure socket layer) technology. This is the same standard underlying the secure form of internet transmissions, ie HTTPS.[10]
- Only the RTS developers know the security key for data encryption. This information should not be shared – even with the institution's personnel.
- The SIM chip in each PoS terminal is programmed to call only one number, the port for the appropriate RTS server. If the chip is reprogrammed to another number, it can not call the server.

RTS Server

RTS Authentication

RTS System

- Authorized administrators of the institution require a password to log into the RTS server. There are currently three levels of access permitted[11]:
  - "User" which allows read-only access to the monitor page
  - "Accountant" which provides User capabilities plus access to the RTS Report Generation and Manual Transaction pages.
  - "Administrator" which allows complete management of the console.
- All three functions require unique passwords. These passwords should be safely guarded by the responsible staff at the financial institution.
- Processes should be instituted to update this password on a frequent basis.
- There is also a timeout built into the system. If there is no activity within that timeout period (3 minutes), the RTS session will close.

Data Encryption and Security

RTS System

- The RTS servers should be set up in their own Demilitarized Zone (DMZ) at the data center. They should be accessible from only one port. This reduces the risk of invasion by viruses or hackers.
- The DMZ should be further strengthened by a firewall that is installed around all the servers to minimize the risk of exposure.

[10] If the most powerful computer in the world today was to try to crack this code, the computer would have to run for 38 years.

[11] In the next version of the software, we are considering up to five levels of access.

- All information that passes between the RTS server and the financial institution's MIS application is encrypted with SSL 128-bit. This is true for both send and receive modes.

RTS Fraud Detection

RTS System

- In order to guarantee that each transaction is processed by the RTS server once and only once, the transmission from the PoS device includes a message number, resend count, and PoSID. The RTS server keeps track of these numbers and expects each PoS to send transactions in sequence. If this does not occur, an error results and the PoS terminal in question can not upload additional data. In normal working conditions, the sequence verification should not cause a problem. Therefore, it is a way to detect potential fraud in the system.

MFI MIS

The majority of security at this level will have to come from operational procedures and the trust relationships that are established between the financial institution and its authorized staff. It will be important for the institution to put processes in place that will allow the organization to have checks and balances for these individuals, especially the RTS Administrator. Over time, the institution should also develop procedures, both electronic and operational, that will allow the institution to analyze transaction flow, fund withdrawals, and other client patterns. This is a current best practice in financial systems, but the solutions in place are too complex and expensive for many smaller financial or microfinance institutions.

MIS Authentication

RTS System

- The MIS server assumes that only the associated RTS server knows its IP address and the port number of the connector. If this information was shared, then a hacker could post transactions directly to the financial institution's server. Therefore, this information needs to be guarded by the RTS Technical Support team.
- To diminish the risk associated with unlawful sharing of the IP address and port number, the RTS system utilizes an encrypted connector which adds another layer of security. Only authentic RTS servers and authorized MIS servers will be able to encrypt and decode data streams that are being sent between the two servers.

Operational Procedures

RTS System

- The microfinance institution’s connector has a “listener” component that waits for the RTS server to tell it what to do. The MIS does what the RTS server tells it to do. One of the things that the RTS server requests is information about account balances and client data. The RTS server does not have a “listener”. Thus the MIS can not request processing from the RTS server.
- The financial institution should put safeguards in place to ensure that no one person has complete control of their system. There need to be checks and balances to avoid internal fraud.

Appendix

Offline Best Practices

Europay:

- PoS devices and ATMs in Europe conduct the majority of transactions in an offline mode and are prompted to initiate an online connection when a parameter is exceeded or periodically for back-end data updating.
- PoS devices in Europe download the numbers for invalid cards. When a client transacts, their card is compared to the list of "bad" cards before they are authorized to proceed.

Stored Value Cards:

- These cards detect limits, provide flags when card is close to the limit, and prevent further activity beyond limit.
- The card is the central point for transaction data updating onto the back-end system and for maintaining data security.
- Transaction data for specific period can be retrieved from the PoS device in case of operator card failure.
- The interaction between the stored value card and a PoS device provides the basis for business logic and detecting limits during transaction.
- The stored value card is required for a transaction and the interaction with the PoS device. This provides a basis for maintaining account balance & tracking account activity.

Visa Horizon, a stored value card:

- Has pre-authorized limits stored on card.
- Accounts are reconciled periodically to enable business management and monitoring.
- At the end of day, the merchant performs a real-time transaction for updating of the back-end.
- Accounts are reconciled periodically to update funds balances within shadow account & initiate changes for primary account
- When the client (or agent) card hits the transaction velocity limit, they have to be connected real-time to get more money downloaded or they have to take their card to the bank.
- When the client card runs out of money, they have to be connected real-time to get more money downloaded or they have to take their card to the bank.

RTS Risk Management Summary

Value Chain Element	Technology	Operational Procedure
Card	Cryptomemory smart cards EMV L1 comliant Card id locked at manufacture Data on card encypted Card linked thru PoS to one user Cards can be disabled	Offline: primary mode of transacting
Client	Linked to card through RTS Pin number required Receipt generated Last 10 transactions stored on card	Relationship established at branch Card disbursed at branch Pin assigned at branch Teach confidentiality of pin Require pin and second form of id * Future option: photos or fingerprints Savings account minimum balance Limit number transactions per day Limit amount per transactoin Client signs agent receipt Requirements for online transacting Disable card if lost or stolen New pin number provided at branch New clients build savings history
Agent	Linked to card through RTS Linked to 1 PoS device through RTS Pin number required Receipt generated Last 300 transactions stored	Financial institution responsible for agent integrity Agent must hold savings acct at financial institution Card and PoS distributed at branch Savings account minimum balance Limit value of daily transactions Agent signs client receipt
PoS Terminal	Card locked to PoS decive (offline) Card linked to PoS device (online) PoS name linked to device id RTS port number coded into PoS Encryption key coded into PoS	Train one agent, one device
Data Transmission	Serial via authorized staff only Each transaction separate packet Packets encrypted via SSL-128	Agent responsible for phone bills

	bit Key limited to development team SIM chip calls RTS server only	
RTS Server	Password protected access System timeout feature DMZ environment with one port Data in and out encrypted Inbound with counter/message num	Update procedures for password Select timeout period
MIS Server	Only RTS server knows IP & port Encyrption used thorugh connector	Control of RTS to be divisional Procedures need to be developed