RTS Version 3.3

OPERATIONS GUIDE

This page intentionally left blank

TABLE OF CONTENTS

Introduction

This guide is intended for the executives and managers of microfinance institutions or any other individuals who are interested in a high level overview of the Remote Transactions System or RTS. It is an excellent introduction to the RTS for both technical and non-technical staff. Brief descriptions of the other manuals and guides available for the RTS are listed in the Appendix.

Introduction to the RTS

General Introduction

The Remote Transactions System (RTS) was developed by a consortium of public and private organizations[2] convened by the Hewlett-Packard Company in August 2003. The team came together to determine how technology could be applied to reaching a breakthrough in the scale of microfinance. They envisioned the creation of a "transaction processing backbone" that could capture financial transactions wherever they occurred and transmit them to back-end financial systems.

The RTS, the first component of the backbone, was developed specifically for environments where there was limited infrastructure, and specifically for the unique business needs of microfinance institutions. The solution is a combination of technology and business processes that will capture the loan payments, savings deposits and withdrawals of financial clients. Although the original aim of the RTS was to be methodology neutral and adaptable to both group and individual lending approaches, during the implementation of the solution two versions evolved – one for institutions that utilize internal agents and group lending practices (internal agent model) and another for institutions that wish to leverage independent third-party agents[3] (external agent model).

The RTS is composed of a hardware device, known as a point-of-sale (PoS) terminal, a specialized software application, smart cards, and a RTS back-end system. All transactions that are captured on the PoS terminal are uploaded at the end of the day to an RTS server (simple PC). The data then moves through a connector to the accounting systems of the appropriate microfinance institution. The PoS terminal is a mobile device that can run more than 12 hours without a battery charge and in areas where there is no connectivity.

The solution was developed according to financial industry standards. Our purpose is to eventually enable a seamless integration between the RTS and other financial systems. In this way the data collected from the field can eventually be routed into other banking systems, through central switches and into other components of the global financial infrastructure.

From January 2004 through March 2005, the RTS was alpha and beta tested in Uganda. It was also installed and piloted in three microfinance institutions – UMU, FINCA

[2] The Microdevelopment Finance Team (MFT) includes individuals from Accion International, Bizcredit, FINCA International, Grameen Technology Center, Freedom from Hunger, Global eChange, PRIDE AFRICA, and Hewlett-Packard Company.

[3] Both versions will be described in this document. Special notations will indicate where the two versions differ significantly.

UGANDA, and FOCCAS. Each institution used a different model in their implementation of the RTS.

Implementation Models in Uganda

Tracking Individual Clients within Group Methodology

FOCCAS adheres to a group lending methodology and provides non-financial education sessions at their group meetings. Therefore, loan officers must participate in group meetings. When the RTS was implemented, FOCCAS was beginning to track financial information at the individual client level. Previously they had only tracked this data at the group level. Loan officers took the PoS terminal to group meetings where they captured all the loan deposits, savings deposits and other financial transactions. In taking full advantage of the RTS solution, FOCCAS had the opportunity to streamline their group meetings, improve transparency for all parties, and accelerate their reconciliation processes.

Local Sub-branch

FINCA *UGANDA* was piloting the concept of a sub-branch, a low cost branch closer to targeted clients. A FINCA teller would travel to the sub-branch two times a week to collect money from the leaders of the local groups. The teller would take an RTS PoS terminal to the sub-branch where the group information would be captured electronically.

Third-Party Agents

UMU tested the RTS solution with independent third-party agents who would become "human ATMs" or extensions of UMU's business by providing financial services to UMU's clients. These agents were local merchants, or trusted individuals, who have some daily financial liquidity through their business operations. Each agent kept a PoS terminal at their place of business. UMU clients traveled to the agent where they performed their financial transactions, all of which were captured electronically on the PoS terminal. Cash was exchanged between the agent and the client.

When a transaction occurs, the agent is actually distributing and collecting cash. The agent supplies the cash and the microfinance institution or bank's MIS system transfers funds from the client's account to the agent's account, so the client account is debited for the funds they received and the agent's account is credited with the amount they just transferred to the client. When a loan payment or deposit is made by the client, the reverse backend accounting occurs. In these cases, the client account is credited and the agent's account is debited because the agent has received cash, as if the agent made a withdrawal from their account. Debiting the agent account requires that the agent has sufficient funds in their account to cover the debit.

At the end of the day, all the transactions are uploaded to the RTS back-end through the cellular network. Since the agents were also UMU clients, funds were reconciled nightly through UMU accounting procedures.

Benefits to Microfinance Institutions

The objective of the RTS was to increase the scale of microfinance by impacting four key variables: operational costs, financial costs, capital flow, and industry dynamics.

- Operational costs: The RTS attempted to reduce rural and peri-rural transaction costs for participating microfinance institutions by lowering the cost of their existing operations and the cost of expansion. The RTS also attempted to lower costs for clients by providing a local, convenient place for transactions. Reduced fraud loses can also result due to the increased control over fraudulent transactions and theft that the RTS provides through the electronic capture and management of information.

- Financial costs: The RTS enables the electronic capture of client level transaction data for microfinance institutions. This improves management information and enables more rapid, accurate decision-making and improved performance.

- Capital flow: The electronic capture of client level transaction data is a first step toward improving institutional reporting, which is required to attract additional commercial funding.

- Industry dynamics: The RTS is a first step in fostering cooperation between microfinance institutions and other financial providers on key industry issues and challenges, such as data standardization, transaction security, and infrastructure cost sharing.

Benefits to Clients

The RTS provides finance clients with two key benefits:

- Increased access to financial services: by reducing costs and human resource requirements for finance institutions, the technology should help the acceleration of penetration by finance institutions into new rural and peri-urban markets.

- Reduced opportunity costs for accessing microfinance in the third-party agent model: the pilot network of third-party merchants for local cash disbursement and collection will reduce travel time, and enhance convenience and the opportunity of accessing local financial services.

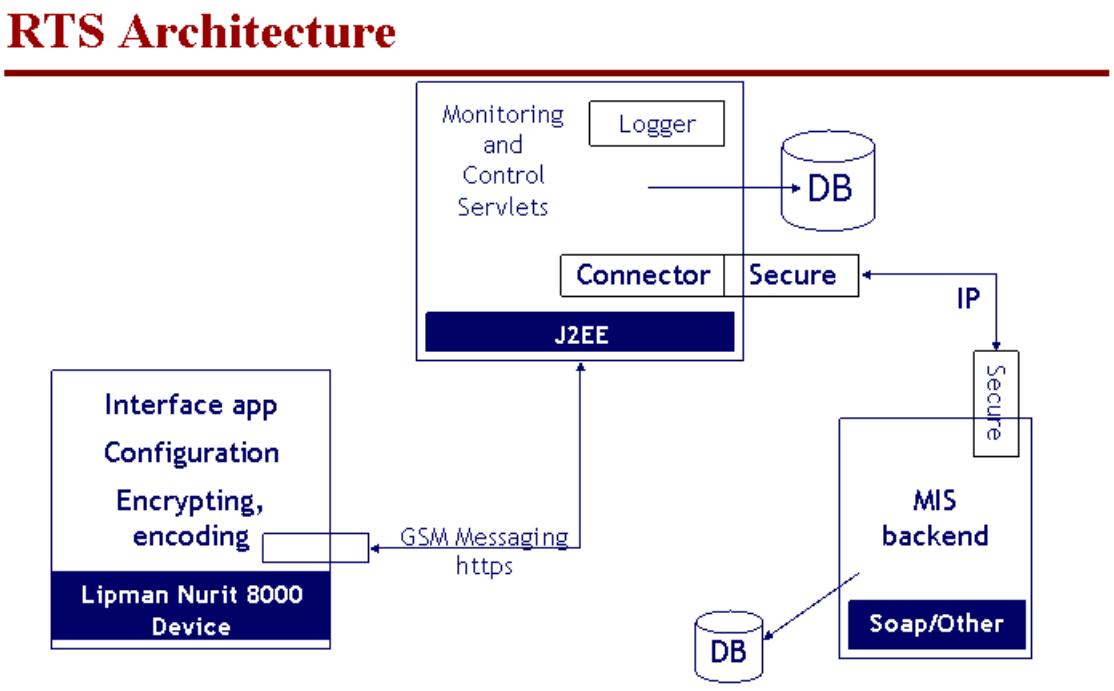
RTS Architecture

Components of the RTS

The RTS solution consists of the following components:

- Smart cards distributed to clients and agents
- Wireless point-of-service (PoS) terminal running the RTS client software
- Centralized server running RTS server software and an MFI connector interface
- MFI accounting system to which transactions are reconciled

The following diagram shows how the main components of the RTS fit together. Although our original intention was to build one connector for all accounting packages, we discovered that we had to build different variations of the connector for each of the microfinance packages that we worked with, in this case Banker's Realm, Loan Performer, and SIEM.



Online vs. Offline Operations

The PoS terminals are equipped to communicate with the RTS Server and MIS backend computers through several different means - via GSM, landline, or serial cable. Real-time transactions can occur through any of these communications means.

Although the RTS was originally developed as a primarily online, real-time system, the realities in Uganda forced us to switch to a primarily offline system. RTS V3.3 has been developed to work in a primarily offline mode. The new solution is more reliable, has lower recurring costs, and is more secure. Online transactions can still occur, but only at the branch office under the control of authorized microfinance staff. There will be a feature in the PoS that is set with the Super Operator card. Once set, this feature restricts agents from performing online transactions.

When connecting to the RTS Server through either GSM or a landline, the PoS terminal is making either a cellular or regular phone call. Both of these approaches are used when the PoS terminal is not in the same location as the RTS Server. If the PoS terminal is in the same location as the RTS Server, then the PoS terminal can be connected directly to the RTS Server through a serial cable.

The client and agent smart cards always have the most recent balance of all their respective accounts. The cards are, in effect, electronic passbooks. When an offline transaction occurs, changes to client and agent accounts are captured on both the smart cards and in the memory of the PoS terminal.

When transactions are written to the client card, they are marked as “Pending”. There can be between 6-7 Pending Transactions kept on a client card at any time. When a client requests an online transaction at the branch, all the pending transactions less than 7 days old will be uploaded to the RTS server. This is done to ensure that the integrity and security of the system. Once the transactions are uploaded, their pending status is removed. The RTS server will accept up to two occurrences of the same transaction. However, the RTS server will send only one occurrence to the corresponding MIS system.

The entries on the PoS terminal memory are known as “Saved Transactions”. At the end of the day these Saved Transactions are uploaded to the RTS Server where they are processed and passed on to the microfinance institutions’ accounting system.

RTS Transactions

Transaction Process

From the client's perspective, a transaction starts with the PoS terminal and the smart card that acts as the client's secure passbook. A brief description of the transaction process follows:

- A client arrives at authorized PoS terminal with their authorized smart card, additional ID if required, and the cash that will be deposited or applied to a loan
- The agent initiates a transaction through the PoS by inserting her smart card into the terminal thus authenticating the terminal and its association with that agent.
- The client inserts their smart card into the PoS terminal.
- The type of transaction – savings deposit, loan payment – is selected.
- The amount of payment is entered into the PoS
- A screen appears requiring both the agent and the client to confirm the transaction type, account number, and amount.
- Upon acceptance of the transaction, the PoS device prints two receipts – one for the client and another for the agent.
- At the end of the day, the agent performs a series of processes that include reconciling their cash on hand with a PoS Summary Report.
- End-of-day procedures also include making a phone call through the PoS terminal. The POS dials out over the cellular infrastructure[4] connecting it to the RTS Server[5]. All stored transactions are transmitted to the RTS server.
- To ensure that the time required to connect to, and communicate with, the RTS Server is minimized, the POS "packetizes" the data it is sending by compressing and encoding the data.[6] The data is also encrypted[7] for security purposes.
- Transactions flow from the RTS server through the connector to the appropriate microfinance accounting system
- Accounting staff at the microfinance institution perform a set of end-of-day reconciliation procedures

[4] The cellular infrastructure is based on the GSM standard. The RTS sends data packets across GSM, using the analog portion of the cellular network. In Uganda, this means that there is less reliability because the cell phone providers give priority to voice calls and will drop data lines when their system is full.
[5] The GSM connection is made with a PPP server at Bushnet allowing the digital packets sent over the analog signal to be forwarded to the proper RTS Server, which is identifiable by its IP address. Phone numbers and IP destinations are hard-coded into the RTS Client software. In the current implementation, each microfinance institution has a unique IP address, since they each have their own RTS Server. A more scalable solution would be to have the data from all participating microfinance institutions collected by the same server. The microfinance institutions in Uganda were not prepared to make this choice because they did not fully understand the technology and were concerned that sharing a server meant their competition would have access to their data, which is not at all the case.
[6] Compression is via built-in "code books" that are shared with RTS server.
[7] The encryption information is hard-coded for added security. It also uses standard encryption techniques for https but no public keys.

Smart Card Authorization

The first step in the transaction process is authorizing and authenticating both the agent and the client. This is accomplished through an interaction between the smart cards and the PoS terminal.

When the client approaches an agent, they must be in possession of their smart card and their Personal Identification Number (PIN). If they are missing either one, they cannot complete a transaction. Assuming the client has arrived with both their smart card and pin, a conversation ensues between the client and the agent during which the client indicates what transactions they want to perform. The agent and the client should count the money to verify that the appropriate funds are present before they even begin the transaction process.

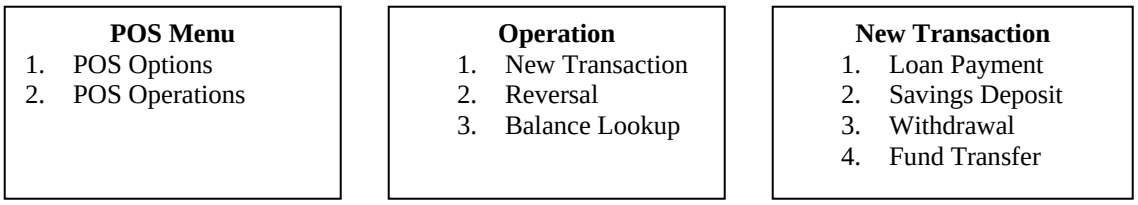
Once funds have been verified, the agent initiates the transaction by inserting their smart card into the device and entering the correct PIN as confirmation. The client then identifies herself by inserting her smart card in the terminal and entering her PIN. This combination of actions builds security into the system by insuring the integrity of the PoS terminal/agent connection. Proper security features in both the RTS system and the operational approach of the microfinance institution is of paramount importance.

After the agent and client have identified themselves properly, the client has the ability to repay a loan, deposit money to savings, withdrawal money from savings, or transfer funds from one account to another. During the process, if an account or amount is entered incorrectly it is possible to correct the error or cancel the transaction altogether. Should one of these transactions be completed before the parties realize an error has been made, it is possible to void the transaction, essentially reversing a previous erroneous transaction. A client may also look-up the balance on any of her accounts from the PoS terminal.

All transactions are conducted in an offline or batch mode. These batch transactions are stored on the PoS terminal until they can be uploaded to the RTS Server. In most cases, uploads should occur at least once a day to ensure accurate reconciliation at the back-end. Literally thousands of transactions can be stored on the PoS terminal before it is full. This provides a great deal of flexibility to the microfinance institutions and their agents, particularly for those situations where transacting needs to occur in remote areas without a stable GSM network.

Transaction Types

A series of three main menus – PoS Menu, Operations, and New Transactions – enable the client to access all of the transaction types currently available through the PoS terminal.



POS Main Menu (agent) POS Operations Menu (client) POS Operations Menu (client)

A complete menu structure for all the PoS options and operations is contained in the Appendices.

Loan Payment

After the client chooses **New Transaction** from the PoS terminal's display menu, the first option is **Loan Payment**. After selecting this option, the client is shown **a list of her loan accounts** on the PoS terminal. After choosing the loan account to which the client chooses to make a payment, she enters the **amount to be repaid**. A summary screen appears confirming the savings account and deposit amount. If correct, the client continues the transaction. Otherwise, the transaction is aborted and the process starts again with the New Transaction menu. If the client chooses to continue the operation, the account balances on the client and agent cards are both updated. Then two receipts are printed, one for the client and another for the agent.

Whenever a transaction is completed, the client has the option of starting another transaction or of exiting the system.

Saving Deposit

After the client chooses **New Transaction** from the PoS Terminal's display menu, the second option is **Savings Deposit**. After selecting this option, she is shown **a list of her savings accounts** on the PoS terminal. After choosing the savings account to which the clients chooses to make a deposit, she enters the **amount to be deposited**. A summary screen appears confirming the savings account and deposit amount. The transaction continue in the same manner described for a loan payment.

Withdrawal

After the client chooses **New Transaction** from the PoS Terminal's display menu, the third option is **Withdrawal**. After selecting this option, the client is shown **a list of her savings accounts** on the PoS terminal. After choosing an account, the client inputs the **amount to be withdrawn**.

Fund Transfer

After the client chooses **New Transaction** from the PoS terminal's display menu, the fourth option is **Fund Transfer**. After selecting this option, the client is again shown **a**

list of her savings accounts on the PoS terminal. After choosing an account from which she wishes to transfer funds, the client inputs the **amount to be transferred**. The PoS terminal then asks the client to identify whether the receiving account is a savings or loan account. If she has more than one account option at this point, the PoS terminal presents the account options to the client. After the transaction is completed by the PoS terminal, in either real-time or batch mode, the client and agent cards are updated and receipts are printed.

Cancel Transaction

The final step of all the transactions described earlier is that the agent and client cards are updated and receipts are printed. Before this happens, however, the client or the agent may press the "menu/cancel" key to cancel the transaction. Reasons for canceling a transaction include choosing an incorrect transaction type or account, or entering the wrong amount. Canceling a transaction before the cards are updated or the receipts are printed is equivalent to the transaction never happening at all since the results of the transaction were not placed in the PoS memory. It is as though the transaction never happened. A new transaction may be started in its place.

Reverse Transaction

A reversal is completely different from a cancelled transaction. In this case a transaction has been completed, stored on the PoS device and ultimately processed all the way through the backend systems. A reversal is a transaction that reverses a previously completed transaction. Although rare, and only possible in an online mode, it might be possible for a client and the branch agent to complete a transaction and then realize that the transaction was incorrect. In such cases, the correct procedure would be to reverse the previous transaction.

To reverse a transaction, first, the client and agent authenticate their identities using their smart cards and PINs. After the client chooses **Reversal** from the PoS terminal's display menu, the client is prompted for the **receipt number** of the transaction to be reversed. After inputting the number, the PoS terminal sends the information to the RTS server which in turn contacts the microfinance institutions' backend. A message confirming the reversed transaction is shown on the screen. The client card and the agent card are both updated and a reversal receipt is printed for both the client and the vendor.

Balance Lookup

The balance lookup is not considered a transaction because no funds are moved and no cards are updated. Balance lookups are conducted in an offline mode and return data from the smart card.

To check a balance, the client and agent first authenticate their identities using their smart cards and PINs. After the client chooses **Balance Lookup** from the PoS Terminal's display menu, the PoS terminal then asks if the requested account is a savings account or

a loan account. After choosing an account, the client is shown the account balance maintained on her smart card. Agents will use a special agent card balance lookup to obtain the balances on their cards.

Authorized PoS terminals at the branch can also be used to lookup account balances on the back-end. When they are at the microfinance branch, agents and clients can use this additional feature to compare the account balances on their cards with the account balances on the back-end systems.

Limits

In the external agent model, the microfinance institution can set a series of limits that provide additional security. This feature is not required when the microfinance institution is using their staff as agents.

Limits include:

- Maximum client withdrawals (amount) each day[8]
- Maximum client withdrawals (amount) before client must visit the branch
- Minimum savings account balance (client and agent)
- Maximum agent receipts (total amount collected) each day

In the external agent model, if the agent's account balance drops to zero, they can no longer accept loan payments or deposits from clients because the microfinance institution can not be guaranteed that they will be able to recoup these funds. This is why there is a minimum savings account balance for agents.

In the internal agent model, the agent balance is not as critical. In these cases, the agent balance should be set at a very high level. When it begins to drop down to zero, the agent card will need to be updated by the microfinance institution to a large value again or the agent will no longer be able to perform transactions across the RTS.

Fees

In the eternal agent model, the microfinance institution can also set transaction fees. These fees are set through the RTS server and then downloaded to the PoS terminal. To change the fees assigned to a particular PoS terminal, the RTS supervisor must reset the fees and then download the new information to the PoS terminal through the "get credentials process".

[8] A day is defined by the microfinance institution as a 24 hour period that begins at XX:XX on one day and ends at XX:XX minus one minute the next day. For example, 18:00 Monday to 17:59 Tuesday. Weekends are considered extensions of Friday. In the previous example, Friday would run from 18:00 Thursday to 17:59 Sunday.

There are two types of fees, account fees which are paid to the microfinance institution and transaction fees which are paid to the agent.

Account Fees

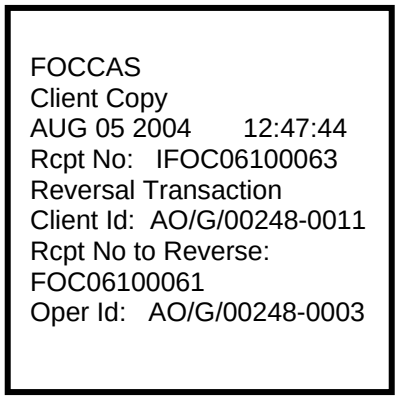
Each type of transaction (deposits, withdrawals, balance lookup) can have its own account fee. These are fees that the microfinance institution deducts from the client account. These fees can be structured as either flat rates or percentages. The same fee will apply to all clients at the microfinance institution. Account fees are available for both the internal and external agent models. When applied, the fees are automatically deducted from the client card before account balances are updated. The agent card balances will not be affected.

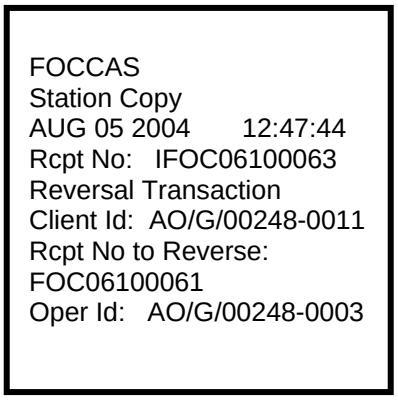
Transaction Fees

Transaction fees are the fees that clients pay the agent to perform their transaction. These fees are only available in the external agent model. Each transaction can have its own fee structure. For example, there may be a charge for a withdrawal, but no charge for a balance lookup. If desired the microfinance institution can change these fees for different agents. When applied fees are automatically deducted from the client's account balance before their card is updated and the fee is automatically added to the agent's account balance before their card is updated.

Receipts

Each transaction results in the printing of a client and agent receipt. The contents of the receipts are displayed below.





Batch transactions have an "I" before the remainder of the receipt number as shown above. The transaction number for an online transaction would not include the "I". Instead it would be FOC06100063.

The PoS Terminal

The PoS Terminal allows agents of a microfinance institution to collect and distribute funds related to savings and loans in a manner that is professional, builds trust with the clients, and helps to ensure adequate accounting and safeguards at the collection end of the system. The first terminal that has been programmed to accept RTS transactions is the Lipman Nurit 8000, a commercially available product of the Lipman Company.

The Lipman Nurit 8000

When the RTS system was initially designed, it was fully understood that the solution would have to work in areas where there was erratic electricity, limited connectivity, potential extremes in temperature, dusty conditions, and with customers that may not have alpha literacy skills. The final cost of the solution was also an important consideration because the RTS would not be replicable at scale if microfinance institutions could not justify its purchase through a realized return on their investment. For these reasons ATMs and PDAs were eliminated as appropriate transacting devices since they did not meet even the basic needs assessment.

The Lipman Nurit 8000 was chosen because it met the following requirements:

- Rugged design and battery power
- Programming interface that could use java runtime builds
- Support and distribution available globally for future usage scenarios
- Built-in GSM capabilities
- Built-in Smart Card reading/writing capabilities
- Built-in Printer

Overhead view of Lipman Nurit Device with test Smart Card

Although the RTS solution was developed on the Lipman Nurit 8000, the software was written with the expectation that it would need to be ported to other devices. The solution should require only minimal alterations to run on other PoS terminals.

Details of the features of the Lipman Nurit 8000 are included in the Appendices.

Additional views of the Lipman terminal provide another perspective on the device. There is an optional cloth holster available for the device that provides added protection and helps the working portions keep freer from dust during times when the device is not being utilized.

Lipman Nurit 8000 in cloth holster from side-top and full side view

The PoS Software

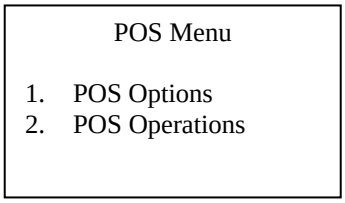
The PoS Software that the client and agent interact with is not the software native to the PoS terminal. The Lipman Nurit 8000 is shipped with a default interface that allows the purchaser to load customer-specific applications developed in Java to the terminal. Before a PoS terminal goes into the field, it must be loaded with the RTS PoS software that converts the terminal into an RTS terminal for a specific microfinance institution.

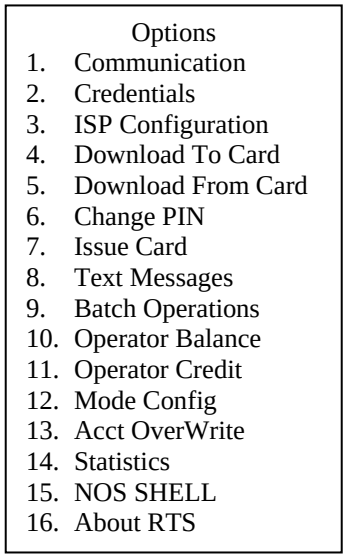
Each POS terminal is registered to a specific microfinance institution and to a specific agent within that institution. The agent can be a loan officer, a teller, or a third-party agent. For security purposes, each PoS terminal can only be operated by one agent. Preparing the PoS terminal for the field requires that it be initialized and credentialed or "authorized".

During the pilot these initialization and credentialing functions were managed by the RTS Uganda technical support team. In the future, these operations can either be contracted out by participating microfinance institutions or the capability to manage these processes can be developed within the microfinance institution's technical support team. Unless the microfinance institution has a sophisticated team, however, it is recommended that these technical support functions be contracted to appropriate personnel.

Agent Operations

In addition to acting as a "human ATM" in the field, the agent has additional responsibilities related to the smooth operation of the PoS terminal. The agent has the ability to configure and troubleshoot the PoS terminal. The figures below show the Main and Options menus that are useful to the agent.





Start-of-Day Operations

The PoS device will check for "saved" transactions that occurred before the close of the previous day. If such transactions exist, the Agent can not proceed with new transactions until they have successfully uploaded their pending transactions.

End-of-Day Operations

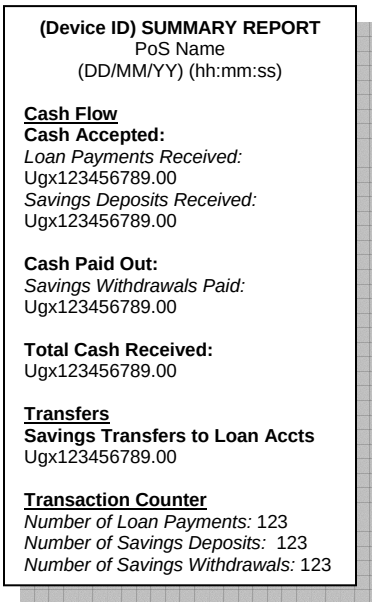
At the conclusion of each day, the agent will proceed through a three step "end-of-day" process. The three steps include:

- Producing PoS Batch Summary Reports
- Uploading all the pending transactions on the PoS
- Retrieving text messages

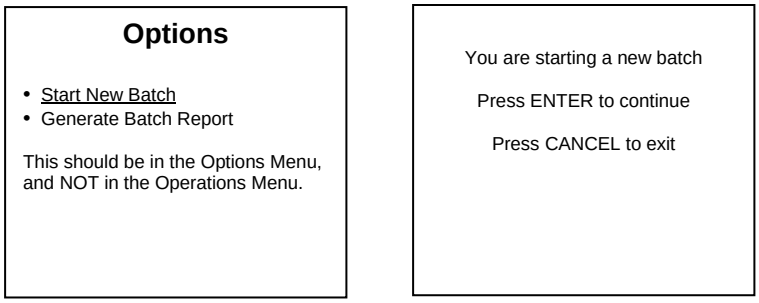
The agent will perform these steps in order through the Options Menu. Text messages are described later in this document.

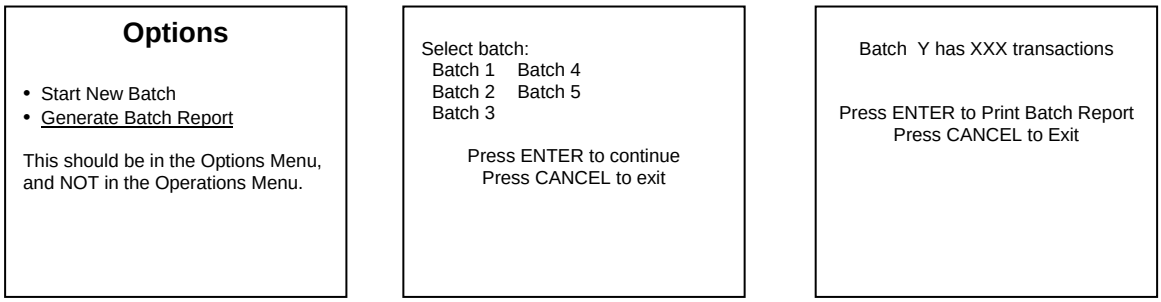
PoS Batch Summary Reports

PoS Batch Summary Reports will summarize all the cash accepted and paid out during the day. This report will be used by the agents to reconcile their cash holdings at the end of the day. A sample of the report follows:



The PoS Batch Summary Report can actually be generated by the agent up to five (5) times during the day, if desired. The process flow is as follows:





In the internal agent model, this feature allows Field Officers to produce PoS summary reports after each group meeting. Thus the Field Officers can work with each group to reconcile their cash. Even if the Field Officer manages five groups in a single day, the information from each group can be managed separately. Similarly Tellers can use this option to check their cash position from time to time during the day.

In the external agent model, this feature allows the agent to produce summary reports before each upload. If the agent is extremely busy during the day and does not want to wait until the end of the day to upload all their transactions, the agent can perform end-of-day processes several times throughout the day uploading the pending transactions that are on the system at that time. Once transactions have been uploaded from the PoS, the information is no longer available in the PoS Batch Summary Reports.

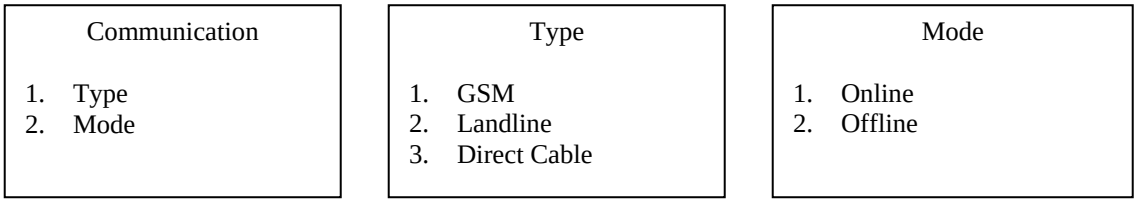
PoS Options Menu

Each of the choices within the PoS Options menu will be briefly described.

Communication

The Communication option allows the agent to choose how the GSM communicates with the RTS Server. If the transactions are collected in the offline mode, they can eventually be uploaded to the RTS server via GSM, a landline[9], or a direct serial cable.

The menus available after selecting the COMMUNICATION option are shown below.



Communication Menu (agent) Type Menu (agent) Mode Menu (agent)

To set the PoS to transact via batch in the field, the Type must be set to ”Direct Cable” and the Mode to “Offline”. To communicate over the GSM network, the Type must be set to “GSM” and the Mode to “Online”. When working via a serial cable, the Type is set to “Direct Cable” and the Mode to “Online”.

Credentials

This option downloads RTS credentials from the RTS Server to the PoS terminal. The credentialing process is another element of the security built into the system.

Each PoS terminal is uniquely matched to a single agent card. The first time the terminal is placed in the field it must be credentialed. This process takes the terminal number and the number of the inserted agent card and matches it to a database on the RTS server. If the match is incorrect or the terminal or card is not yet listed in the RTS server, then the PoS terminal cannot be used.

[9] The landline feature is not part of Version 1.0 of the RTS. Depending on usefulness and need, it may be added to the next version of the system.

If the agent card needs to be changed at a later point in time it is possible to re-credential the terminal via the same process, but it is expected that this process will not be done frequently.

Download to Card

The download to card feature allows saved transactions to be moved from the PoS memory to a high volume smart card that functions as transportable memory. Essentially, the smart card acts as a floppy and can be used to transfer the data to another PoS terminal that is located in an area with connectivity or direct access to the RTS Server. In this way, remote PoS terminals that will never have access to the GSM network can still be effectively utilized. Data is simply moved manually through the high volume smart card to a location where the data can be accessed. The transfer of data from the PoS terminal's memory to a high volume smart card deletes the data from the PoS terminal. The special card used for this purpose has greater memory storage capacity and is discussed later in the Guide.

Upload from Card

The upload from card feature is the complement to download to card feature. After downloading data from one terminal onto a high volume smart card, the card can be taken to another terminal and uploaded. These saved transactions can then be uploaded to the RTS server.

Text Messages

The RTS has the ability to queue up text messages for PoS terminals. At the end of each day when the terminals connect to the RTS server, any text messages that have been sent to the RTS servers will be downloaded by the PoS terminals. The microfinance staff has the option of sending text messages to a specific PoS terminal or they can send a broadcast message which will be downloaded by all the PoS terminals.

The PoS terminals can send text messages back to the RTS server. There is no broadcast ability from the PoS terminals.

NOS Shell

The RTS PoS software runs on top of the Nurit Operating System (NOS). One option available is to access this operation system directly. This would only be used by RTS staff for troubleshooting. The option is password and operationally protected.

About RTS

The About RTS option shows the version of the software being run and other information about the PoS software installation. This data is useful to the RTS technical support team when they are troubleshooting problems related to the terminal.

Smart Cards

There are two types of smart cards used in the RTS solution, a 2KB memory card that is used by clients and a 32KB card that is used for agents, super operators, or as a floppy[10]. Client cards can hold approximately 6-7 transactions and the high volume cards can hold up to 300 transactions. As a result, the high volume cards can be used as floppies or as a backup transaction log.

Client Card

The client card is used by the client as a secure passbook. With their card and their PIN number, the client can make deposits, withdrawals, repay loans, and transfer funds. Part of the client training is teaching the clients the importance of keeping their card secure and their PIN secret. After a successful transaction, the client card contains new account balances.

The client card contains client numbers, account numbers, account names, account types and account balances as well as a number of special codes built into the cards for security purposes. This data can only be altered using a PoS terminal through a regular transaction or through special applications that were developed to manage the cards. These special applications – the touch-up program and the mass writer – are described below. Several security features have been put in place to prevent the unauthorized alteration of this data. Inconsistencies in the data are checked when the transactions are uploaded to the RTS server.

Agent Card

Agent cards are high volume 32KB cards. Agent cards contain the same type of account information that the client cards contain because the agent's accounts need to be verified and updated for each transaction. The account information on the agent card is not as critical in the internal agent model as it is in the external agent model. However, it will be necessary for each microfinance institution to create an "agent" account in their accounting systems. For those institutions using the group lending method, this agent can be set up as a bogus client account. All the agent needs is a valid ID and savings account number.

On all agent cards, there are also unique values that link each card to a specific agent and to a previously specified PoS terminal. If the card has not been credentialed to a PoS terminal, it will not work on that terminal. This is true even in batch mode as there is a message, or cookie, coded into the PoS terminal during the credentialing process that ties it to a specific agent card.

[10] Card part numbers are AT88SC1616C and AT88SC25616C for the client and agent cards respectively.

For each transaction, the agent is required to insert their card and enter their PIN. Each credit to a client account results in a debit to an agent account and vice-versa. If either account has insufficient funds to complete the operation, the transaction is not allowed. At the end of a successful transaction, both cards are updated with the new balance of their accounts[11].

Super Operator Card

The Super Operator card is a high volume smart card (32KB) that provides an authorized user with special capabilities. There are two types of Super Operator cards – device and card. Device Super Operators are able to change settings on the PoS such as IP addresses and online/offline mode settings. Card Super Operators are able to issue or reissue client smart cards. A specific Super Operator card can be programmed to manage both devices and cards, if the microfinance institutions chooses to set the cards up that way.

Online/Offline Capability

There will be an on-off switch accessible through the Options Menu that will set a PoS device to online only, offline only, or mixed modes. Once set to offline only, the PoS can not accept online transactions. This switch will be used to force agents to transact in offline mode.

Overwrite Account Balances

A Super Operator card will have to be used at the branch to update client or agent smart card balances. This functionality will be in the Options menu. This super-operator function will simply display account information, such as account name and type, for all accounts on the card. Then, the Super Operator will choose which account balance needs updating. The current card balance will be shown and the Super Operator will be able to enter the new balance below it. This action will write the new balance to the card and send a confirmation of the amount written.

Floppy Card

A high-volume smart card (32KB) can be used as a floppy. Transactions can be downloaded from a PoS terminal on this card and transported physically to another location. Transactions can also be transferred from the card to a PoS terminal.

[11] This last point has important implications for microfinance institutions wishing to use the internal agent model. In some cases, the MFI's accounting software can not handle the creation of an "agent" or "teller" account. In one version of the RTS solution agent transactions are held on the RTS terminal and never sent to the MFI's accounting software.

Smart Card Initialization

Client and agent smart cards must be initialized and credentialed before they can be used in the field. The process of producing valid smart cards requires the following four steps:

- Print card with microfinance institution's design and client data
- Program the card with client specific information, such as account numbers and balances. Cards are programmed through either the mass writer application that enables hundreds of cards to be produced very rapidly or through a TouchUp application that reads, writes, and edits smart cards one at a time. These programs reduced the total cost of smart cards by 50% for participating microfinance institutions.
- After the cards are programmed, they are credentialed through the RTS Server.
- Once the cards have been initialized and credentialed, they are ready to be distributed to the clients and agents.

Smart Card Software

In the process of developing the entire RTS solution, a cost-efficient solution to "programming" the smart cards became a priority. Two programs were developed that would allow the RTS Uganda team and/or the microfinance institution to program critical data onto the agent and client cards. Another application was developed to test the PoS terminal under high volume conditions. This is known as the PoS Stress Tester.

TouchUp Application

The first of these applications, the "TouchUp" program, has the ability to read, write, and edit the content of both agent and client cards. Through this application, the following information can be programmed on a card-by-card basis:

Institution Code	Client Code	Client Number	
Account 1 Number	Account 1 Name	Account 1 Type	Account 1 Balance
Up to 3 additional accounts may be stored and an associated transaction counter with each account			

The TouchUp program is used when a card needs to be modified, when new clients are being added to the RTS implementation in smaller batches, when a client gets a new loan or in other similar situations. The TouchUp application is also very useful to the RTS Uganda team as a troubleshooting tool. The TouchUp program is secured with a 10+ digit PIN number and should only be handled by authorized staff.

Super Operators can also print transactions that are stored on either client or agent cards. It is possible to print the entire card contents, only the personal information about the client, or only the transaction history.

Mass Writer Application

The second application, the "**Mass Writer**" program, enables the microfinance institution to create literally hundreds of smart cards very quickly. This application is used when the microfinance institution is adding lots of clients to the RTS implementation. To use the mass writer application, a PoS terminal is connected via serial cable to a computer that contains a database containing all the card information. This database is created from the excel spreadsheets that microfinance institution staff develop each time they wish to add clients to the RTS implementation.

PoS Stress Tester

This application automatically drives a high volume of transactions from the PoS terminal to the backend system to test new versions of the software or in other test modes. The application can be set up to run a variety of transaction types. The applications resides on a POS device and does not need any other special requirements.

Back-End Functionality

RTS Server and MFI MIS PC Configuration

To maintain reliability, the RTS Servers and the MFI MIS computers must be placed in a location that has stable electricity, connectivity and security. The systems also need to be maintained by a team of technology specialists. In Uganda, RTS Uganda identified Bushnet as a local vendor that could provide the technical environment and support needed for the microfinance institutions. Refer to the Appendix for a diagram detailing the hardware configuration at Bushnet.

Bushnet has a special relationship with MTN, Uganda's second largest telephony provider. Through a licensing agreement, MTN has allowed Bushnet to piggyback its signals on its trunk lines and to use its communications towers to create a unique wireless network, which has been incorporated in the overall RTS solution for Uganda.

The configuration of the RTS Server and MFI's MIS PCs at Bushnet was developed to maximize both the ability to scale the solution and to ensure the greatest stability of the system. All three RTS Servers are located at Bushnet. The computers are placed behind a firewall[12] to ensure their security and keep them free from viruses, which can pose a tremendous challenge in an unstable technology environment.

All calls from the PoS devices enter into the RTS system through the GSM network, identified as the GSM tower. These data streams then pass through a firewall at Bushnet. The information streams from the PoS devices are routed to the appropriate RTS Server based on the IP address that was passed with the data stream. The data that flows into the RTS server is then passed to the appropriate MIS system. In the case of FINCA UGANDA, this is SIEM 7. For FOCCAS, the MIS application is Loan Performer. And for UMU, Banker's Realm.

Since the electrical reliability of FOCCAS' Mbale branch was not adequate, the FOCCAS MIS PC was permanently located at Bushnet. The Mbale branch has been equipped with thin-client terminals, which have very low electrical consumption, and a wireless antenna that allows staff to access their accounting system in Bushnet. This solution has greatly enhanced the FOCCAS' ability to access their server 24 hours a day, 7 days a week, if desired. It also dramatically reduced their Internet connectivity costs at the same time.

During the pilot, FINCA *UGANDA* and UMU had parallel servers located at Bushnet that ran their accounting product, SIEM. As the pilot proceeded, the pointer from the RTS server at Bushnet was shifted to point to the production MIS servers in FINCA and UMU's branch offices. In some cases, special firewalls were required to provide security

[12] Cisco Systems PIX firewall 520

for the data transmissions between the RTS server and a distantly located accounting package.

RTS Software

The software components that are contained within the back-end of the RTS solution are the RTS Management Console, the RTS-MIS Connector, the MFI MIS applications, and the MIS database containing client account information.

RTS Management Console

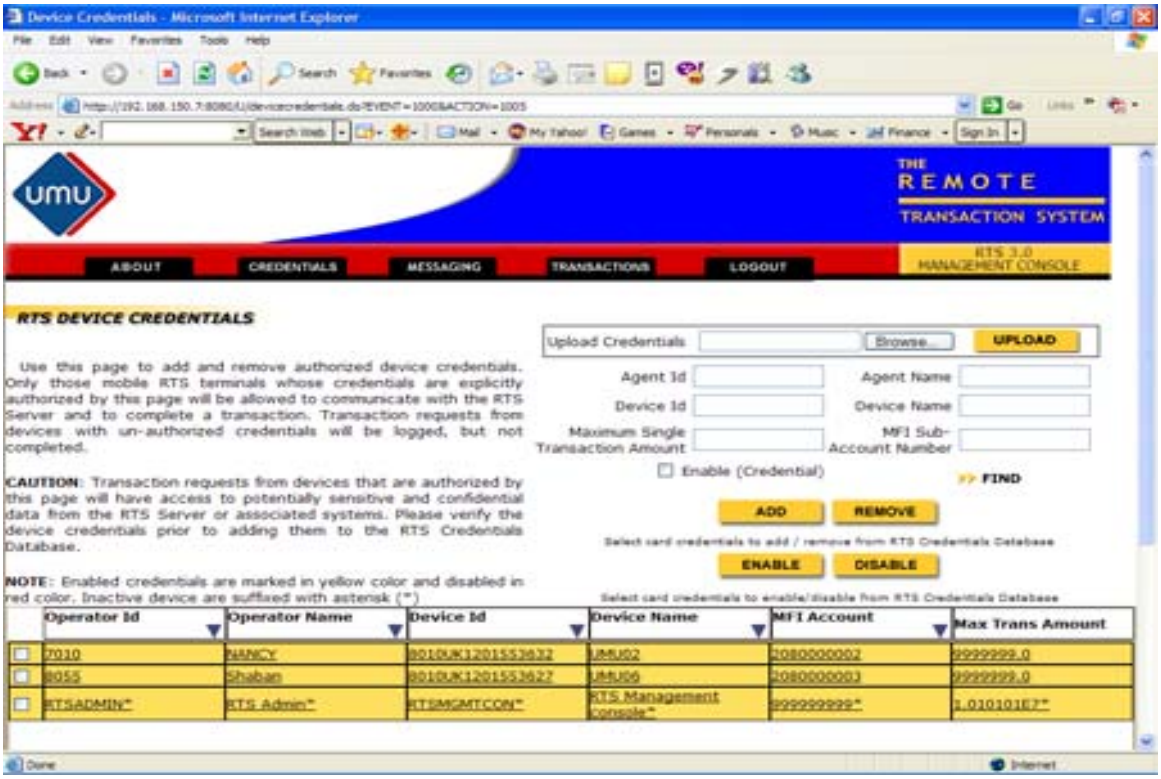
The RTS Management Console (Console) is an Internet web site consisting of an Apache Web Server and a MySql database. For the pilot project, each microfinance institution has a dedicated Pentium PC running Windows 2000, which contains both the RTS Server and Console[13]. The Console provides the following capabilities to microfinance institution users and administrators:

- Login screen requiring password
- Multiple levels of user access (general user, accountant, and administrator[14])
- Card credentials input and control (enable, disable, add, remove)
- Terminal credentials input and control (enable, disable, add, remove)
- Credentials reports for cards and terminals
- Produce detailed transaction reports through the report generation tool
- Manual transaction entry
- Commission and fees setup

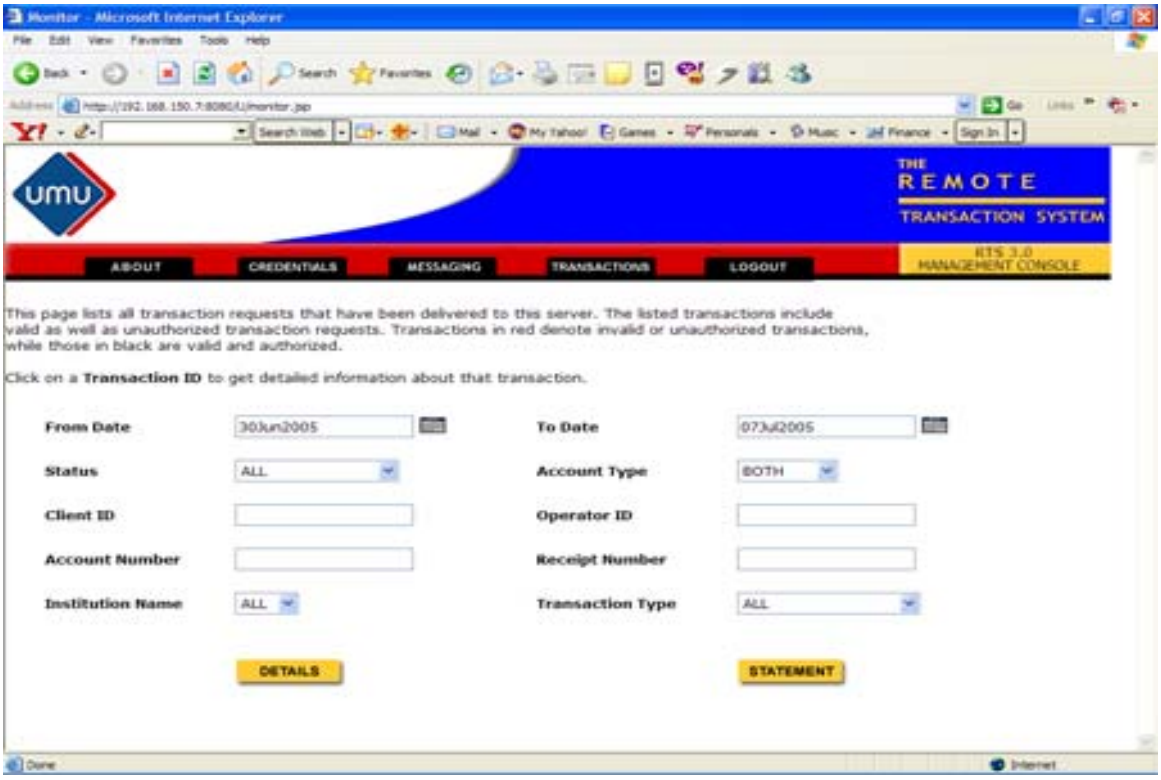
The main Console looks like the images provided below. The first image shows the Console in the RTS Device Credentials page.

[13] The participating microfinance institutions insisted on having their own servers because they did not understand that a single server could provide the same solution at a lower cost while maintaining the integrity and confidentiality of their institutional data.

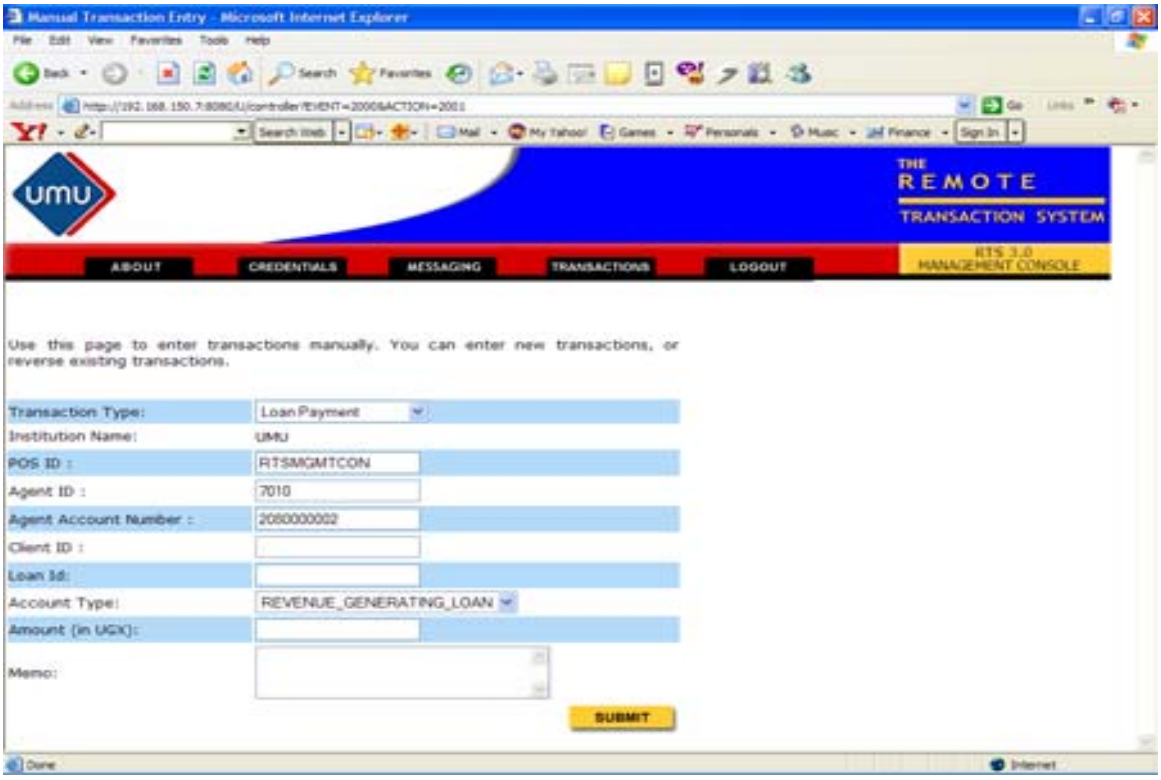
[14] The user can view the transaction monitor. Accountants have access to the Report Generation and Manual Transaction pages. Administrators have access to all functions.



This second screen shot of the Console shows the Transaction Monitor page, which allows the MFI Administrator to create Query Reports from the RTS Server.



The third image shows the Manual Transaction page, which allows the MFI Administrator to manually enter or alter a client transaction. This option will be used by the microfinance institution to correct errors, manage reconciliation, and enable transactions in special circumstances such as the loss of a client card.



The Connector

The connector consists of a TCP application (or server) on the RTS side of the solution and a Listener on the MFI MIS side. The TCP Server manages the sending and receiving of data between the RTS Web Server and the Listener. The Listener manages the sending and receiving of data between the TCP Server and the MFI MIS software. In other words, data that is collected on the RTS Server from the PoS terminals in the field needs to be transferred to the MFI's MIS database. Since the computer running the RTS Server and the computer running the MFI MIS system do not have to be physically connected, or even in the same physical space, the data must somehow be "passed" between the two machines. This is accomplished by the connector, a piece of software that resides on the RTS Server and another piece of which resides on the MFI MIS computer. The MFI MIS side of the connector has to be built by the MFI MIS vendor. For the pilot, there were three vendors involved in connector development – Crystal Clear (Loan Performer), Craft Silicon (Banker's Realm) and MFSI (SIEM).

The original concept was for the RTS Server was to send data streams that were uniform for each MFI MIS system. The MIS vendors were then to build an interface to their

software that would translate the RTS data into a format that their program required. They were asked to build their side of the connector to accept generic data. However, in the process of working with the vendors it became necessary to adapt the RTS-side connector to provide data streams that were unique to each MIS application. This resulted in three flavors of the RTS-side connector. Although the "customized" approach the RTS team ended up adopting simplified the development process for the MIS vendors, it has added significant complexity to the RTS solution. In addition, the approach is less replicable because it makes MIS vendors who want to adapt their systems to accept RTS data more dependent on the RTS development team. As a result, future versions of the RTS connector may revert to the original generic design.

Due to the inherent challenges of reliably and securely passing data between two computers that are not connected, the TCP Server and the MIS Listener are two of the most important parts of the RTS solution. The ability of a microfinance institution to set up these servers, the necessary firewalls, and other security features in a stable, fault-tolerant environment will be very important to a successful implementation of the RTS solution.

Hardware

The original design of the RTS was to have a single RTS server processing the transactions for all the microfinance institutions and then routing them to the appropriate MFI MIS computers. During the initial phases of implementation, the microfinance institutions raised concerns about the privacy of their client data if it was placed on a server with their competitors' data. Although these concerns did not reflect a thorough knowledge of technology and should not have been an issue, RTS Uganda agreed to provide separate servers for each institution. It was just easier at the time. However, it is recommended that microfinance institutions be educated about this issue because they will experience significant cost savings if they share the expenses related to the back-end of this solution, ie the RTS server, support and maintenance costs.

The servers used in the pilot were Pentium 4, 533 Mhz with 512 DDR and 2 80 GB hard-drives. The computers at Bushnet operate on a standard power supply instead of a server power supply, which is important because it reduces costs. While most servers cost several thousand dollars each, the RTS system has been developed to run on regular low-cost PCs with an average price of approximately $1100. This approach brings the total cost of the solution down, and is especially important as the solution begins to scale requiring additional computers.

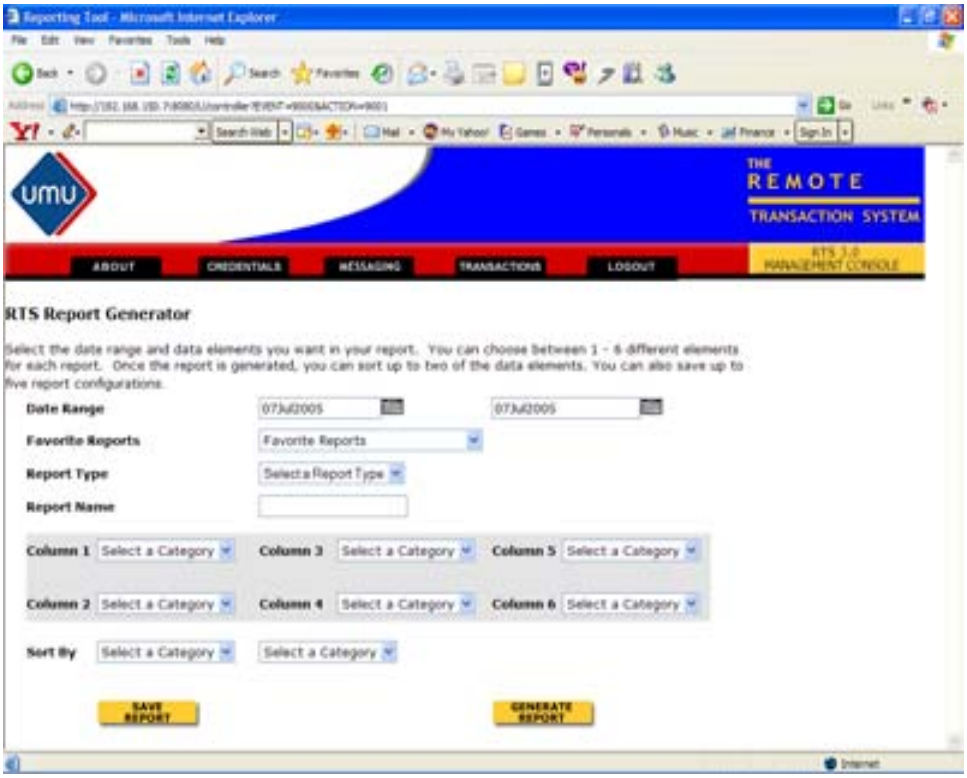
Reconciliation

Each microfinance institution involved in the pilot had a unique approach to their reconciliation process. The approached depended on a combination of current institutional practices, their accounting and GL software, and the quality of the connector that was built by their MIS vendor. The RTS Uganda team worked with each microfinance institution and their vendors to use the RTS as a means of simplifying and improving the efficiency of their reconciliation procedures.

Report Generation

A Report Generation Tool was developed on the RTS Console to provide accounting staff with the greatest flexibility in producing RTS reports that would most closely match their internal accounting and GL reporting mechanisms. The Report Generation User Interface provided on the RTS Console is shown below. This is followed by a description of the tool as well as a sample report.

Report Generation User Interface



Element Selection Process

The RTS Administrator will select the date range for the report. When the Start Date is entered into the tool, the End Date will automatically shift to the Start Date. Thus if the report is only for one day, the admin will not need to do anything else. If the report will cover a range of dates, then the admin will change the End Date content.

The RTS Administrator will have the choice of selecting from a group of up to five (5) saved report formats. These are intended to be formats that the admininstrator uses frequently. Selecting from this list will minimize the need to recreate favorite reports each day. Once a favorite report is selected, the report will be generated.

If the admin does not choose a saved report, then they will have the option of selecting a Report Type. Three types of reports are available:

- Agent ID, one agent is specified
- Client ID, one client is specified
- Transaction Type, one transaction type is specified

The administrator will select the elements required in the report. One element of the 15 available can be selected for each column. As few as one or as many as six columns can be produced in the final report.

The administrator will be able to determine a primary and secondary sorting choice. For example, the primary sorting criteria within an agent report might be “PoS Timestamp”. “Client ID” would then be sorted within each date range. Any of the data elements can be either a primary or secondary sorting element. It is assumed that all alphabetic data will be sorted alphabetically. And it is also assumed that all numeric data will be sorted from smaller numbers to larger numbers.

The administrator also has the choice of naming the report.

If the administrator wants to save this report format among the favorites, they click on the “Save Report” button. If there are less than 5 saved reports, the new report is automatically saved. If there are already 5 reports, the admin must choose the report that will be replaced by the new saved report.

Finally, the “Generate Report” button will be selected to create the report.

Report Generation

When the report is generated, it will include the report name, date range, report type, date, time, and page number. Each column will have the name of the element selected for that column at the top of the column.

Column Titles should be in bold, without the "_" in the names, each word in starting in Caps. All elements except "amount" should be left-aligned.

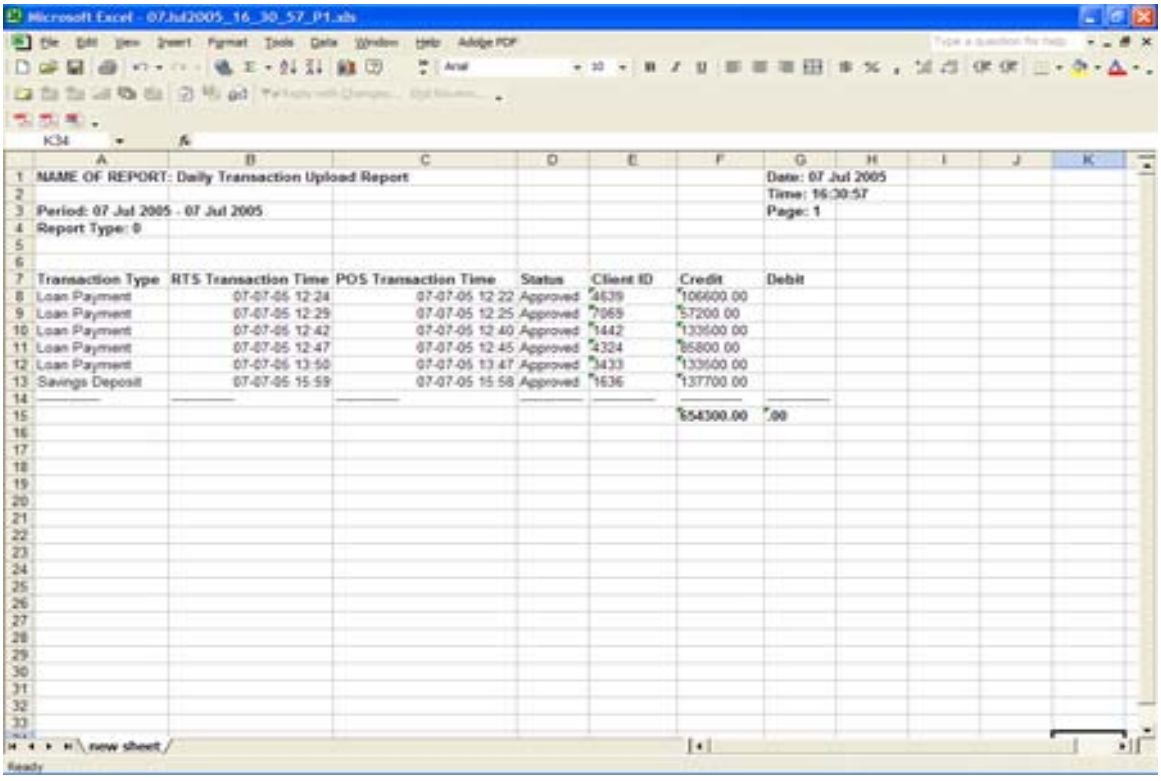
Amounts should be right-aligned. Amounts should reflect Ush. There needs to be enough room in the amount columns to accommodate a high shilling amount. This is particularly true of the totals.

Times will adhere to the military, 24-hour clock. Dates will be presented in dd/mm/yy format.

When the "amount" element is selected for one of the columns, two columns will be generated labeled "Credit" and "Debit". Transaction amounts will show up in the appropriate columns. These amounts will be totaled at the bottom of the report.

Once the report has been generated, the administrator will have the ability to print the report directly from the HTML or the report can be exported to MS Excel.

Sample Report



	A	B	C	D	E	F	G
1	NAME OF REPORT: Daily Transaction Upload Report						Date: 07 Jul 2005
2							Time: 16:30:57
3	Period: 07 Jul 2005 - 07 Jul 2005						Page: 1
4	Report Type: 0						
5							
6							
7	Transaction Type	RTS Transaction Time	POS Transaction Time	Status	Client ID	Credit	Debit
8	Loan Payment	07-07-05 12:24	07-07-05 12:22	Approved	4639	106600.00	
9	Loan Payment	07-07-05 12:29	07-07-05 12:25	Approved	7069	57200.00	
10	Loan Payment	07-07-05 12:42	07-07-05 12:40	Approved	1442	133500.00	
11	Loan Payment	07-07-05 12:47	07-07-05 12:45	Approved	4324	85800.00	
12	Loan Payment	07-07-05 13:50	07-07-05 13:47	Approved	3433	133500.00	
13	Savings Deposit	07-07-05 15:59	07-07-05 15:58	Approved	1636	137700.00	
14							
15						654300.00	.00

Security

Security of financial transactions is a much larger concern in the external agent model than it is in the internal agent model. The RTS Risk Management Guide provides a comprehensive description of the technology features that have been built into the RTS solution for security purposes. The guide also describes recommended operational procedures that a microfinance institution should follow if it wants to minimize its risk as a result of the solution.

Risk management is an ongoing issue that will increase as the solution is scaled. Therefore, it is important that participating microfinance institutions incorporate a set of risk management and audit policies to continually update and improve the security of the solution in their organization.

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[15] and finally, establish countermeasures for appropriate responses to security breaches. [16]

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 be performed by each microfinance institution through its current screening practices of potential clients, which will not change in this system. It 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

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

money that can be withdrawn in any given day, and enabling the managing microfinance institution to withdraw privileges from an agent or client when deemed necessary.

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

Detection

Detection refers to a series of procedures that can be used to alert an MFI 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 most microfinance 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 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 the senior risk management team at VISA, 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 each microfinance institution rolls out the use of the RTS, it will be imperative that the 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.

Refer to the RTS Risk Management Guide for details on risk management through the RTS solution.

APPENDIX

A. RTS Guides and Manuals

RTS V3.3 OPERATIONS MANUAL

The RTS V3.3 Operations Manual will be the manual to use to gain an understanding of the features and functionality of the Remote Transaction System. Intended primary for the management team at Microfinance Institutions, this manual will describe all the components of the RTS solution, including the point-of-sale terminal, the RTS server, the MFI servers, and smart cards. It will also help prospective microfinance users understand the interconnection between the various elements and what is needed to implement the RTS solution in their organization.

RTS RISK MANAGEMENT GUIDE

The RTS Risk Management Guide describes the security aspects of the RTS solution, particularly as it applies to the third-party agent model. This document describes the security features built into the technology. In addition, it identifies the operation procedures that a financial institution should follow to minimize their financial risk through the solution. As the product is taken to scale, this document will require updating and modification.

RTS TRAINER'S MANUAL

The RTS Trainer's Manual is intended for the Training Manager and trainers within a microfinance institution. The manual will provide these individuals with step-by-step instructions on the use of the point-of-sale device and the RTS server. With this manual, trainers will have all the tools they need to train microfinance staff, the RTS system administrator, agents, and microfinance clients on the use of the device. In addition, this manual will include a section that will help agents and trainers troubleshoot problems that occur in the field.

RTS AGENT'S QUICK REFERENCE GUIDE

The RTS Agent's Quick Reference Guide is a laminated fold-out that reminds RTS Agent's of the basic steps they need to follow to manage and maintain the point-of-sale terminal. The guide will include simple step-by-step reminders of the transaction processes. It will also include basic troubleshooting and PoS maintenance recommendations.

MICROFINANCE CLIENT'S QUICK REFERENCE GUIDE

The Microfinance Client's Quick Reference Guide is a fold-out document that will be given to each microfinance client that uses the RTS solution. The guide will be a quick reminder of the steps that the client must follow to perform financial transactions. Based primarily on graphical descriptions, the guide will be useful even to those clients that are not fully literate.

RTS FIELD SUPPORT MANUAL

The Field Support Manual describes a number of potential challenges that might be encountered by an MFI that implements the RTS solution. Examples of problems, along with recommended solutions, include loss of smart cards, loss or destruction of PoS terminals, PoS printer malfunctions, and so on. This manual should be used by the MFI as a template to develop their own internal procedures to handle operational challenges that might arise through the integration of the RTS system and PoS terminals in their organization.

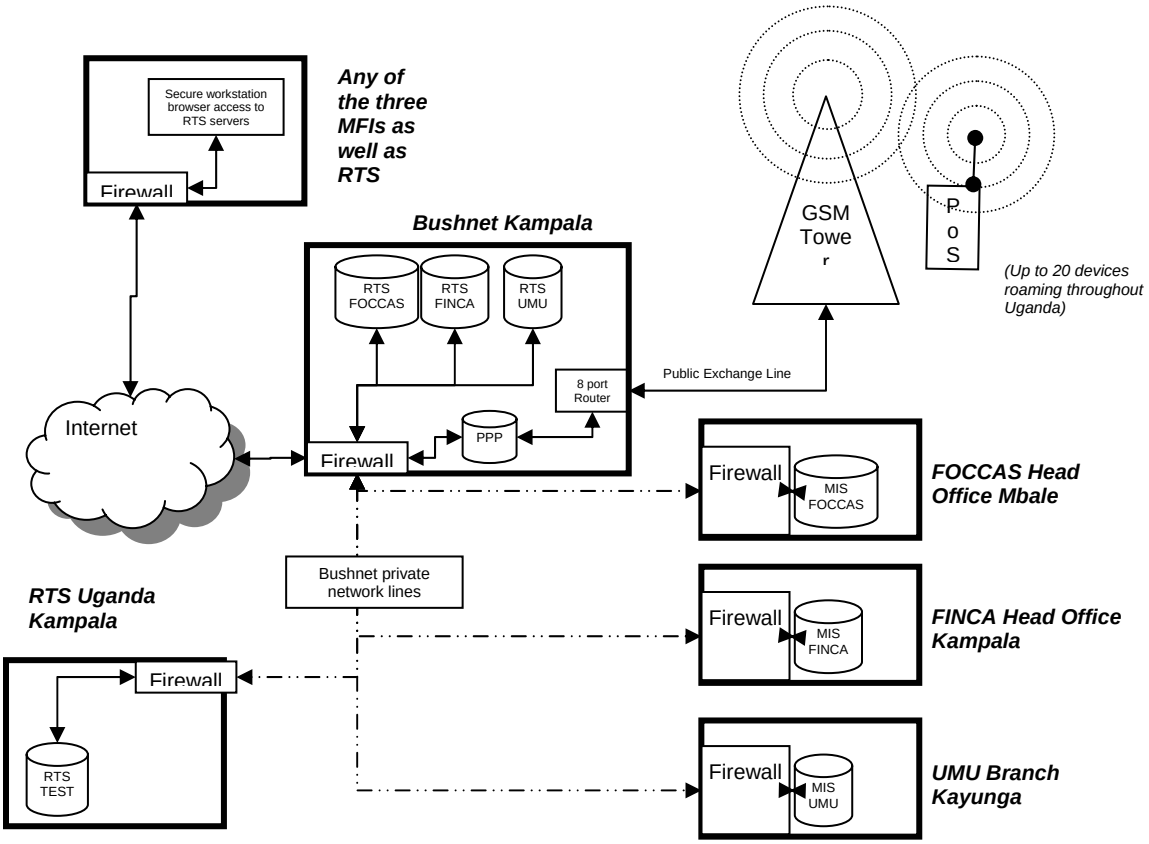
RTS TECHNICAL SUPPORT MANUAL

The Technical Support Manual will contain step-by-step instructions for the technical staff maintaining and supporting the RTS solution. Another key feature of this manual will be the troubleshooting sections which will help support personnel resolve problems that arise with the system based on past experience. This manual will be a work-in-progress with new information being added, especially to the troubleshooting sections, as that information becomes available.

RTS DEVELOPER'S REFERENCE

The RTS Technical Specifications will be the detailed technical documentation for the RTS solution. This document will contain source code documentation, process information, and data structures. It will be used by IT developers and other IT professionals that will seek to implement, enhance or install the RTS in financial institutions.

B. RTS Server and MFI MIS Configurations



C. PoS Terminal Menus

PoS Menu

1. POS Options
2. POS Operations

POS Options Menu

1. Communication
    1. Type
        1. GSM
        2. Landline
        3. Direct Cable
    2. Mode
        1. Online
        2. Offline
2. Credentials
3. ISP Configuration
    1. ISP Phone Number
    2. ISP Username
    3. ISP Password
    4. ISP IP
4. Download to Card
5. Download from Card
6. Change PIN
    1. Chance PIN
    2. Replace PIN
7. Issue Card
    1. Issue New Card
    2. Re-Issue Card
8. Text Messages
    1. Read Message
    2. Send Message
9. Batch Operations
    1. Start New Batch
    2. Close Batch
    3. Print Batch Report
    4. Upload Transaction
10. Operator Balance
11. Operator Credit
12. Mode Config
    1. Lock in Offline
    2. Lock in Online
    3. Offline/Online

4. Online-Only

13. Acct OverWrite
14. Statistics
    1. GSM
    2. Landline
15. NOS SHELL
16. About RTS

POS Operations Menu

1. New Transaction
    1. Loan Payment:
        1. Working Capital Loan
        2. Back to School Loan
    2. Savings Deposit:
        1. General Savings
        2. Personal Savings
    3. Savings Withdrawal:
        1. General Savings
        2. Personal Savings
    4. Fund Transfer:
        1. General Savings
        2. Personal Savings
2. Reversal
        1. Input Receipt Number
3. Balance Lookup
    1. Loan Balance
        1. Home Loans
        2. Study Loans
    2. Savings Balance
        1. General Savings
        2. Personal Savings

There are also a series of menu options specifically for the use of the RTS Technical support team. For detailed information on these capabilities, refer to the RTS Technical Support Manual.

D. Lipman Nurit 8010UK Features

The following are some of the features in the Nurit 8010UK PoS terminal and other terminals in Lipman's 8000 series. The list is not a complete specification of the device.

Human Interface

- PDA sized back-lit graphical LCD display
- Touch screen
- 18-button ergonomically-designed keypad
- Dual track bi-directional tracks 1 and 2 magnetic card reader
- Built-in ISO 7816 Smart Card Interface

Printer

- Quiet, graphical thermal printer ; fast 12.5 lines-per-second
- Easy-load paper mechanism
- Standard 21/4" (57 mm) wide paper, 24/40 characters per line
- Out-of-paper detection
- Multi-language character/font support

Communication Capabilities

- Wireless
- Built-in radio modem
- Internal antenna
- Hardware and software support for a wide range of cellular networks:
- GSM dual-band (optional tri-band) with headset connector for use as mobile telephone
- Dial-up modem at up to 14.4 kbps for telephone communication (33.3 kbps optional)
- Up to two accessible ISO 7816 SAMs located under the battery pack
- TCP/IP protocol support for wireless, telephone line and direct cable applications

Programming Features

- Multi-Application Operating System
- Backwards compatible with existing NURIT applications
- Software Development Kit (SDK), easy-to-use API, application libraries and debugging tools
- Compressed application downloading via radio modem, IrDA, RS-232 or phone line

Power

- Internal rechargeable Li-ion battery pack with protection circuitry
- 12 hours of general operation or over 200 transactions per charge
- Car charger option
-

Additional Features:

- RS-232 port for external terminals
- Dimensions: 82 mm/3.23" (H) x 108 mm/4.26" (W) x 230 mm/9.06" (D)
- Weight: 600g/1.3 lb, including battery pack and paper roll
- Cloth holster with transparent plastic keypad cover available

NOTE: This feature list has been modified from the Acrobat (.pdf) brochure available on www.LipmanUSA.com.

E. Card Processing Software Features

"Mass Writer" program

Card Processing Software. This application enables the programming of hundreds of smart cards, quickly and efficiently. The software will take the agent through the following steps:

- Data for each client (account, PIN, institution, etc) can be typed into the PC-based program manually or can be imported from a spreadsheet
- If the data is in a spreadsheet, each row will represent a new client, while each column will represent various information fields of each client (row)
- One conversion program per each MFI will be provided that converts the desired comma-separated value (CSV) format output by a spreadsheet into the CSV format required by the Card Processing Software
- The data together with the program will be compiled and downloaded into the POS terminal
- For each client string of data, the POS will prompt the agent to insert a new card
- The card will be programmed and verified
- Agent will be prompted to remove the programmed card and to insert the next card to be programmed

"Touch-up" Program

Add functions to the RTS system that supports issuance and re-issuance of smart cards. This software is either controlled by the RTS technical support team or by authorized microfinance institution staff. The program will:

- Add a new type called super-operator, in addition to the standard client and agent types
- Add new transactions to the POS that are available only to agents designed as super-operators
- Issue, reissue or update new agent and client smart cards[17]
- Issue new PIN numbers and change current PIN numbers
- The RTS Management Dashboard will have a page that supports importing CSV (comma separated value) files (e.g., from MS Excel) of all clients/accounts whose cards can be issued or re-issued. This CSV file will be imported into the RTS and displayed on a page for the RTS Administrator with a symbol denoting those cards that have already been issued and a number of times each card has been re-issued.

[17] All card issuance/re-issuance POS transactions need to be credentialed through the RTS Management Console

GLOSSARY

Account Number: (1) A unique series or group of digits used to numerically identify each cardholder. (2) The unique identification number assigned to the account of a specific party, within a given institution.

Agent: A person who is accredited by the microfinance institution and equipped to collect loan payments, collect savings and disburse withdrawals from **Client** savings accounts.

Authorization: *see Credentialing*

Back-End: The data capture and processing activities that occur once a transaction has been captured in the field. The back-end of the RTS includes the RTS Server, the RTS Management Dashboard, the RTS-MIS connector, the MFI MIS application, and the MIS database containing microfinance institution client account information.

Batch Mode: A means of transacting in which data is not passed between the PoS terminal and the RTS Server. Rather the transaction information is captured and stored on the PoS terminal until such time as the data can be uploaded to the RTS Server. Both agent and client cards are updated.

Borrower: *see Client*

Branch Accountant or Central Office Accountant: Authorizes the disbursement in the information system and on paper to trigger the release of the loan from the list of approved loans signed by the **Branch Manger.**

Branch Manager: Performs credit scoring and approves or disapproves loans, maintains the list of approved loans.

Branch Officer: Person who works at the Branch Office and has cashier responsibilities, can process Account Cards, and disburse authorized loans.

Center or Village Group: Larger group, often called a "center", or **Village Group** that consists of 5 or more groups. Usually does not exceed 200 and often around 25 borrowers.

Client: A person who has obtained a loan or savings account from the MFI

Credentialing: The process of authorizing a smart card or PoS device through the RTS Server.

Display: The small screen on the terminal that displays messages to guide users through different operations and to alert users when errors or problems occur.

Field Loan Agent: Loan agent who works in the field (not the office) for the local microfinance institution's branch office.

File: A collection of related data (for example, a batch of transactions is a file).

Fraud Control: Measures taken to prevent unauthorized use of a smart card.

Front-end: The data capture and transmission processes with which the microfinance client and agent interact. In the RTS solution, the front-end includes the PoS terminal, the PoS software, and the smart cards.

Group: MFI sponsored group of borrowers who are organized to support loans and provide social collateral. Group size varies from dramatically from as few as 5 people to more than 40.

Group Leader: Person elected by group to lead meetings, and represent group to MFI or the Center/village meeting.

GSM: GSM is a cellular network standard used in most parts of the world.

Keypad: The key panel used for entering data and performing operations.

Loan Committee: Approves or disapproves loans.

Manual Transaction: Transactions in which account information is entered directly through the RTS Server Management Dashboard (a.k.a. the website)

MFI: Microfinance institution

PIN: Personal Identification Number. A four- to sixteen-digit confidential code or electronic signature used by the card holder to identify himself to the host computer as the proper user of a smart credit.

PoS Device: see *Terminal*

PPP Server: A standard Point-to-Point Protocol for establishing access to a server via an IP tunnel.

Real-Time Transaction: A method of transacting in which the PoS device is communicating with the RTS Server and the MFI MIS software during the transaction. Information is passed directly from the MFI MIS software to the PoS device.

Reversal: see *Void*

Serial Port/Cable: A connector used to communicate with host computers, other terminals, printers, or other peripheral devices such as check readers or bar code readers. The PoS Terminal is connected to a PC via a Serial Cable.

Server Management Dashboard (SMD): The secure website that allows control for credentialing of cards and devices, reporting for transactions, and creation of manual transactions.

Terminal (often called a device): A device used to perform transactions. The transactions are processed by the terminal itself or by a host computer. These devices have a display panel, keypad, card reader and modem, and are used to enter transaction information.

Vendor: *see Agent*

Void (in PoS, also referred to as a Reversal): A monetary transaction used to eliminate a transaction in the current open batch. If the printer is enabled, a void receipt will be generated to be included with that batch's drafts and tickets.

Wireless: A processing mode in which transaction data are transmitted via radio frequency signals instead of via a dialup telephone connection. Wireless transmission requires that the terminal's modem be activated on a wireless network and a wireless gateway. The gateway routes the transaction via a wireless network to the processing host. When the gateway receives a response from the host, it transmits it back to the terminal via the wireless network.