



SWITCHWARE®

Enterprise ATM/POS Transaction Processing and Management System

Overview

SWITCHWARE® is an enterprise transaction processing and management system that provides ATM driving and management plus POS transaction acquiring and merchant management. In a typical environment, SWITCHWARE® provides in-house control of an ATM network, POS terminal support, an interface to a core financial system, connectivity to regional, national or international EFT networks (i.e., MasterCard and Visa) and ATM/debit card management. Other functions include interfaces to a hardware security module (HSM) for cryptographic functions and other applications such as CSF International's u/SNITCH™ automated alert notification system and MIS Reporting System.

The primary purpose of the system is to perform transaction processing and routing decisions. Functions include sending on-us transactions to a primary authorizer, switching foreign transactions to EFT networks, performing PIN validation, standing in when the primary authorizer is unavailable for authorization and performing processing decisions according to predetermined financial institution settings.

General Functions

- In-house ATM driving, management and POS terminal support.
- On-line interface to a core financial system for authorization.
- Stand-in authorization when the core financial system is unavailable for authorization.
- ATM/debit card file management.
- Gateway interfaces to regional, national and international networks (i.e., Visa and MasterCard).
- Interfaces to ancillary applications for alert notification, MIS reports, credit card management, mobile top-up telephone or Internet banking systems.
- Supports industry-standard data security methods including DES, 3DES, MACing, PCI DSS, PA-DSS and verification functions such as CVV, CVC and AVS.
- Interface to a hardware security module (HSM) used for secure key storage and cryptographic functions.
- Currency conversion functions.

Business Benefits

- Provides autonomy in controlling your own in-house ATM network.
- Eliminate third party transaction fees to process at-us, on-us transactions.
- Generate increased fee income from acquired transactions at your ATMs.
- Implement new products and services in a timely fashion without third party involvement.
- Accumulate MIS information to determine usage trends, view transaction types and activity levels, plan for future ATM deployments, determine cash replenishment schedules and average amounts withdrawn at ATMs.
- Personalize your service through system functions including; VIP limits, personal express cash, marketing messages on ATM receipt and customer notes section.
- Superior price/performance and return on investment.

System Architecture

The system utilizes a client/server architecture where the on-line processing is performed on a UNIX or Linux-based server and the user interface is supported using Windows-based workstations. This approach combines the reliability, system scalability and price/performance associated with today's leading UNIX and Linux server architectures with the familiarity and ease of use associated with a Windows for daily user functions.

Scalable Transaction Processing Engine

Financial institutions of all sizes can take advantage of SWITCHWARE®. From community banks to large service centers, the system can be configured to meet existing transaction processing rates and later scaled to meet future growth requirements. Platform support may range from a dual CPU, dual core entry level server to an enterprise level server.

Intuitive Windows Graphical User Interface

User operations including ATM network monitoring, system administration and card file inquiries are conducted at client workstations located throughout the financial institution's LAN/WAN network. The graphical user interface is intuitive and requires little training. The structure is presented to the user in a file tab structure that simplifies the look and organization of data. A variety of built-in functions include drop-down lists, pop-up hints, data entry validations and context sensitive on-line help that simplify the operation of the user interface. Users can perform transaction log queries and produce on-demand transaction and MIS reports.

Relational Database

Application data resides in a relational database providing easy access to system data through SQL queries. Popular industry programs and utilities can also be used to easily extract data from the system.

Rules-Based, Table-Driven and Highly Parameterized

The system is table driven and highly parameterized providing flexibility without hard coded changes. The rules-based capabilities enable each customer to tailor the system

to meet their individual needs. Special processing rules provide transaction processing customization without impacting the core system. As a result, the future introduction of new software updates or releases is not compromised.

High Availability

SWITCHWARE® can support a variety of system configurations specifically tailored to guard against system disruptions caused by a hardware malfunction or natural disaster. Some popular high availability techniques include:

- Disk mirroring (RAID Level 1). Two drives store identical information so that one is a mirror of the other. For every disk operation, the system must write the same information to both disks.
- Disk arrays (RAID Levels 3, 4 and 5) supporting data recovery.
- Multiple servers interconnected to a SAN.
- Real-time data replication supported by the relational database software.
- Automatic switchover techniques and cluster management at the operating system level.

Other high availability strategies may be provided by your Telco provider including frame relay switchover from a production center to a remote standby disaster system.

Multi-Institution Support

The typical SWITCHWARE® configuration supports a single financial institution. However, the system can also be configured to support multiple financial institutions with proprietary ATMs and card issues. In a multi-institution configuration, the system may provide a combination of the following functions:

- Unique ATM loads for each institution.
- ATM monitoring and card file access that is restricted to each institution's data.
- Built-in security features that enable each institution to maintain control over their proprietary data.
- Separate authorization links to independent in-house core financial systems.
- Intra-bank switching between member institutions.
- Settlement reports.

Transaction Validation and Switching

The main function of SWITCHWARE® is to interrogate incoming transaction messages and perform validity checks and routing decisions. Functions include:

- Acquiring and authorization of at-us, on-us transactions, with routing of foreign transactions to regional, national or international networks.
- Processing issuer transactions from regional, national or international networks.

- Unattended continuous transaction processing, with stand-in authorization when the primary authorizer is off-line.
- Stand-in authorization using a negative, velocity or positive card file. A Positive Balance File (PBF) may be utilized to limit the financial institution's exposure to overdrawn accounts.
- All transactions authorized in stand-in mode are stored and then forwarded to the host authorizer when it becomes available.

Transaction and Event Logging

All ATM and POS transactions processed through the system are stored in a transaction log. The transaction log also incorporates system management events such as system startups, cutovers and ATM loads. A query builder function within the System Monitor client application enables a user to perform searches of the transaction log by field or value and display the results electronically. The data presented may be sorted in a variety of formats.

There is a purge function that enables a system administrator to define how much data will be stored in the transaction log before it is automatically purged.

Transaction Authorization

On-Line Authorization

In an on-line authorization environment, SWITCHWARE® performs card and transaction validation before sending the transaction to the core financial system for authorization. If none of the institution-defined limits are exceeded during the validation process, SWITCHWARE® sends the transaction to the core financial system for primary authorization.

Stand-In Authorization

A financial institution can elect to have SWITCHWARE® authorize transaction requests during periods when the core financial system is unavailable. During these periods, known as stand-in authorization, SWITCHWARE® may utilize one of several authorization techniques depending on the level of protection desired by the financial institution. These include:

Positive Card File Authorization

Authorization against a positive card file provides the highest level of card management functionality. A positive card file record contains card processing limits and options that may be specifically tailored to the cardholder. Some of these functions include special VIP processing limits, open account relationships and express cash.

Positive Card File Authorization and a Positive Balance File (PBF)

While in stand-in authorization mode, a PBF may additionally be utilized to limit the financial institution's exposure to overdrawn accounts. The PBF may be updated to reflect the latest account balances. PBF update methods include:

- Real-time dynamic update from the core financial system.
- Periodic batch update.

- Manually via the Customer Card Management (CCM) client application.
- Updated balance returned in the last response message from the core financial system.

SWITCHWARE® will deny a transaction during stand-in processing if the financial account shows an inadequate balance on the PBF. The CCM client application includes a PBF inquiry that allows users to view an account's current and available balance as well as the last financial transaction conducted against the PBF.

Negative File Authorization

This method employs a hot card file that is used to determine whether a card may or may not be used to conduct a financial transaction. If a card is presented that is listed on the hot card file, it will be rejected or captured. A negative file provides the least amount of limit checking during stand-in authorization periods.

Velocity File Authorization

Financial institutions that do not want to maintain a card file but want some level of transaction limit checking can employ velocity file authorization. This method combines negative file authorization with pre-defined transaction limits and privileges. If a card is presented that is not on the negative file, the system will check the limits and privileges for the defined cycle period.

Store and Forward (SAF)

Periodic handshakes determine whether the core financial system is on-line and available for real-time authorization. During periods when the core financial system is unavailable, a transaction request that does not violate any of the limits or privileges contained in the card file will be authorized by SWITCHWARE®. When handshakes determine that the primary authorizer is again available, all authorized transactions are automatically forwarded to the core financial system as force post items.

Security

System Access

A multi-layered security scheme is employed at the operating system and application level. Each user attempting to gain access to the system must enter a valid user ID and password. Customizable user permissions determine the accessibility and functions available to each valid user. The permission levels determine whether the user will have access to the specific client application, and if so, whether the access will include inquiry only or full editing capabilities.

Once access is granted to the system, there are audit tracking functions for the following activities:

- Changes made to the system configuration parameters and customer records. This audit history identifies the exact change made, date and time of the change, and the user making the change.
- Commands issued to the system, ATMs, authorizers, and switches. This audit history identifies the commands by type, date and time,

device(s) involved, and the user executing the command.

- Changes made to the user profile client application that governs access to system data and functions available to users.

The audit histories can be scanned in their entirety, or selectively searched using any combination of the fields as search keys.

A valid user is also notified by the system to enter a new password when the existing password is about to expire.

DES and 3DES

Popular industry standard data encryption techniques including DES and 3DES are supported.

Message Authentication Code (MAC)

Message authentication to ensure that the data in messages sent between two entities has not been tampered with is supported.

Card and Address Verification

CVV and CVC card verification schemes and Address Verification (AVS) are supported.

PCI DSS and PA-DSS Compliance

The system incorporates techniques to protect sensitive cardholder data including triggers that remove sensitive cardholder data from stored transactions and masking sensitive cardholder data in the system's client applications. Additional techniques including data encryption are also supported.

Hardware Security

A hardware security module (HSM) provides secure, tamper-resistant storage of the keys used in performing cryptographic functions and SWITCHWARE provides interfaces to many popular industry models.

ATM/Debit Card File Management

The Customer Card Management (CCM) module provides powerful control over your cardholder's ability to conduct transactions and also provides the ability to limit the risk of overdrawn accounts during periods of stand-in processing. Card file functions include:

- Multiple card issues for each financial institution defined on the system.
- Open account relationships where a single card has the ability to access multiple accounts of the same account type.
- Individualized transaction limits where multiple cards can access the same financial account with different withdrawal limits.
- Unique transaction permissions that govern card usage for a particular financial account. Different cards accessing the same financial account may be established to conduct a unique set of transactions for the same financial account.

- Institution BIN default limits and privileges are created and automatically inserted into new card file records. These default limits can be changed to meet the needs of each individual customer.
- Each card file record includes name and address information, limits, privileges, and accessible financial accounts. A chronological transaction history and free-form notepad function are also provided.
- Time saving card file record duplication and replacement functions.
- Card file queries may be conducted by cardholder number, account number, first/last name, reference ID (i.e., social security number or driver's license number) or other ID. Other ID provides a search by specific data in the card record.
- A card extract client application produces a file of card database information that is used for card encoding and embossing. This file can be transmitted to a plastic card manufacturer for new card production.

The CCM Module supports ATM and debit cards including support for magnetic stripe and integrated chip cards.

ATM Module

This module provides ATM terminal driving and broad support for the industry's most popular ATMs. ATMs can be driven in their native modes, optimizing their capabilities. They also can be uniquely loaded and controlled from a centralized location.

ATM module functions include:

- Multiple ATM types can be driven in their native modes.
- Selective or group downloads can be sent to the ATM network.
- Multiple languages and currencies.
- NCR Electronic Journal (EJ) and Diebold Electronic Data Capture (EDC) upload.
- Coin dispensing.
- TCP/IP, leased line or dial-up support.
- Surcharging (by ATM or transaction type).
- Fraud prevention techniques.
- ATM supervisory functions including supply replenishment, new business cycle, updating host totals, printing cash position and terminal totals.
- Settlement reports.
- EMV smart card support
- Remote key loading
- No envelope cash-in and check-in deposits

ATM terminal handlers include:

- Advanced NCR NDC

- Advanced Diebold 91x
- Wincor Native NDC
- Wincor Native 91X
- NCR NDC+
- Diebold MDS/912
- Diebold 910/911
- Triton proprietary format
- ISO 8583
- Visa II

ATM transactions include:

- Inquiries
- Withdrawals
- Transfers
- Deposits
- Payment enclosed
- Fast cash and personal express cash
- Full and mini-statements
- Checkbook and statement request
- Coupon and stamp dispensing
- PIN change
- Loan and utility payments
- Messages to the bank
- Cash-in and check-in

The system also integrates with Paragon Application Systems' ConfigBuilder™ utility enabling ATM configuration files and receipts to be built from a desktop computer. ATM screen and receipt layouts are easily built and edited with point and click technology. ATM program screen flow can be reviewed without the use of an actual ATM.

System Monitoring

Full monitoring and control of your ATM network is provided by the System Monitor client application that can be run on any client workstation. Devices and authorizer connections are represented by different icon. The icons are color-coded to indicate the communication or operational status at a glance. For each node you can access current status and configuration data, as well as status and transaction histories.

The System Monitor also provides various ATM, authorizer, and switch commands. With proper security, you can issue commands to the ATM network or download ATM terminal programs. Commands may also be issued that take an authorizer off-line or initiate a dynamic key exchange with a network. Functions include:

- Full network command and control, including system startup and shutdown; bringing ATMs in and out of service; downloading ATM terminal programs; initiating dynamic key exchanges with

ATMs and switches; sign-ons, sign-offs, and business day cutovers for switches; etc.

- Graphical monitoring of direct connect ATMs from client workstations, including cash and supply positions, current and historical terminal statuses, communication history and transaction totals.
- Graphical monitoring of host authorizers and switches, including current and historical communication statuses.
- System activity monitor shows current transaction processing rate, as well as a graph of the volume over a predetermined period of time.
- Flexible on-line electronic journal searches of the transaction log including the ability to query on dates, amounts, card number, transaction type and void code with a sort function that organizes the resulting matches in the desired order.

POS Module

This module is available for financial institutions that desire the ability to directly control a POS terminal network and provide merchant settlement and reporting. The module serves as a front-end mediating communication between the POS terminal network and the authorization application(s).

POS module functions include:

- Merchant file containing merchant data.
- Multiple POS terminal types supported.
- Current and historical transaction totals are kept per POS terminal.
- Settlement transactions from the POS terminal are supported.
- TCP/IP, leased line or dial-up support.
- Settlement reports.

The following application formats are used to perform POS terminal driving.

- ISO 8583
- Visa II

POS transactions include:

- Purchase
- Purchase reversal
- Purchase with cash back
- Refund
- Refund reversals
- Funds available inquiry
- Settlement transaction from terminal
- Tips

Available through credit cards:

- Preauthorization
- Preauthorization reversal
- Void sale

- Offline sale
- Offline refund
- Sale adjustment

Transaction Reporting, Settlement & Reconciliation

All transaction activity processed by SWITCHWARE® is recorded and tallied in daily reports. These reports are produced for each financial institution, at the time of day defined by the financial institution.

The transaction reports are broken down into summary and transaction detail to facilitate balancing with the ATMs, core financial system (host) and network (switch).

The ATM reports track transactions over the ATM balance cycle, show on-us and foreign activity, and include suspense reports for both the institution and networks. Host reports track transactions over the institution's business day, and show on-us transactions acquired at the institution's terminals separately from on-us activity acquired by switches. Switch reports track transactions over the EFT network's business day, and organize on-us and foreign transactions in separate reports.

ATM Supervisor Functions

When SWITCHWARE® detects that an ATM supervisor card has been inserted into any ATM in the network, a special set of ATM screens are displayed that help facilitate cash balancing.

Automated Reconciliation

A reconciliation subsystem is available to assist in reconciling transactions originating from other sources from application sources against SWITCHWARE's transaction log. Any discrepancies are quickly identified for easy reconciliation.



CSF International ... What The World Is *Switching To*

For more information, please contact:

CSF International, Inc.

1629 Barber Road
Sarasota, Florida 34240-9392 USA
Tel. +01.941.379.0881
Fax. +01.941.371.5223
www.csfi.com
sales@CSFi.com

SWITCHWARE and VOLTDS are registered trademarks of CSF International, Inc. u/SNAC and u/SNITCH are trademarks of CSF International. Windows is a registered trademark of Microsoft Corporation. ConfigBuilder is a trademark of Paragon Application Systems.

© 2010 CSF International, Inc. All Rights Reserved. Version 6