

Overview of Real-Time and Merchant Server for ITE

The Merchant Server solution replicates the Visa and MasterCard design, implementation and deployment model from both a technical and business perspective, and with regard to the 2010 compliance standard. There are 2 primary components to the program. Merchant Server as the central server providing hosting, validation and central processing all ITE claims, and the IPOS device as the remote client to enforce machine validations independent of POS or cashier and submission of ITE claims, in real-time. With hundreds of functional components and protocols contained within the system, Merchant Server is a very complex device, with over 10 years of design poured into it.

1. The Merchant Server:

In addition to the database server, there are five major server components within Merchant Server. These components handle all aspects required of an ITE program including the following: Communications, Transmission, Encryption, Digital signature, Key publishing, Pin Number validation, Database access, Interfacing, Server switching, Load balancing, Clustering, Database replication, Backup, Reporting, Error logging, and Auto recovery. Also included is Messaging (various messaging protocols and file transmissions), etc. and of course the ITE claim validation and processing.

To "simply" describe the workflow of a normal ITE claim transaction at the server:

- ADR Server manages multiple forms of communication (dedicated, VPN, internet, dial-up) and protocols (TCP/IP or UDP native, AES, SSL), handle and accept for connections
- Upon connection, Agent Server issues public keys to be used in conjunction with stored private keys for data and Pin Number encryption, and digital signature (AES Macing)
- ITE claims are submitted by IPOS and arrives at the Server(s) via various form of communications handled by ADR Server
- Agent Server provides validation of encryption and digital signatures, including eligible Merchant ID
- Decrypted data is dispatched by "switching " to one of the less busy Process or Application Servers (load balancing), or to alternative physical server (clustering)
- The Process Server validates data format, and the submitted data detail, and processes the ITE claim based on pre-configured validation rules. It sends a request to Agent Server for Pin Number or alternative validation requirements, if it is needed. If additional validation is required, it will respond with a "conditional rejection" and prompt for the required validation data. If the validation data or Pin Number is present, it will submit to and be validated by the Agent Server.
- Once validation is completed, the Process Server will apply ITE specific validations, including ID, amount calculations, claim limits, and so on, and sends the "final approval", "partial approval", or "conditional rejection", "final rejection", requested "information" like balances or totals
- The response data is encrypted by Agent Server, carried via ADR server and returned back to the IPOS device

There are two dozen other potential "message" or "file" oriented services provided by the Server to IPOS device, like server messaging, eligible product update, tax rate update, history reports, configuration download, firmware download, etc. Each within has multiple sets of communication

protocols and error recover mechanisms. They are handled by the hosted Application Server instead, and dispatched during "switching"

2. IPOS device

The purpose of the IPOS device is to provide a machine enforced validation without any dependency on the POS or the cashier. Additional validations other than the initial card swipe will be directly between the Server and the individual on a dedicated "PinPad". The details are masked, which isolates the information from the operating clerk or POS.

To "simply" describe the workflow of ITE claim transaction at the device:

- The Cashier swipes the ID card, IPOS validates it based on applicable device validation rules
- IPOS makes the connection to Merchant Server via a pre-configured form of communication and protocol,
- IPOS obtains and validates public keys issued by Merchant Server
- IPOS formats the ID along with the Merchant ID and other information, as a "validation" request (pre-authorization)
- IPOS encryption of the formatted data using the combination of public and private key, and generates a digital signature using the combined Macing key
- IPOS submits encrypted validation requests and waits for the Merchant Server response
- At the same time (IPOS to Merchant Server communication is in the background), IPOS will continue to accept product entries for the ITE claim, validating eligibility and exemption amount. IPOS will perform a device based product validation, i.e. UPC when scanned or when UPC is manually entered, or fuel volumes when integrated into electronic pumps.
- Upon completion of the entry, IPOS will format the final ITE claim
- If the initial validation requires additional validation or Pin Number, it will prompt and ask for the information directly from the individual, masked and isolated from the cashier or POS. The additional validation data will be formatted as part of the transaction data. In the case of the Pin Number, it will perform additional tasks and encryption's as required by Agent Server. Actual Pin Number is not transmitted at all.
- If the Server approves the entire transaction, IPOS will be prompted and produce a detailed receipt, optionally to be printed for manual claims
- If Merchant Server partially approves, i.e. overlimit, IPOS will alert and print the overlimit receipt
- If Merchant Server responds with a "conditional rejection", IPOS will prompt and obtain additional validation rules or calculations
- If Merchant Server rejects the claim, IPOS will prompt to either void, or complete the transaction. If it is to complete the transaction, IPOS will produce a detailed receipt, optionally to be printed for manual claims
- If communication fails due to an error transmission, up to 3 full attempts will be made, each including a request for public keys, re-encryption and so on.

- If communication fails at Server, it will re-attempt at the failsafe server
- If communication fails at ISP, it will re-attempt at the alternative ISP connection
- If communication fails at a dedicated line, it will re-attempt using dial-up if possible
- If communication fails at a local device or network to the line, it will prompt clerk's attention
- If all communication attempts fail, it will use a pre-configured local validation rule and engage SAF. Upon each successful communication, it will automatically submit SAF transactions via "Force-Post" in the background
- Each ITE transaction takes a minimum of 3 communication sets to complete, the card validation, the ITE validation, and the approval capture (or void/rejection). In case of overlimit or validation rejection, the ITE validation make take 5 communications before Server issues final void/rejection)
- Upon any ITE initial action at IPOS (Mag-stripe Swipe, SmartCard Insert, Laser Scanning, or Key Entry), IPOS will perform "pre-dialing" to establish a secure connection in the background. Upon completion of an ITE transaction, IPOS will hold the connection for 3 to 5 minutes (so called "line-camping" or "keep-alive") ready for immediate and fast ITE processing. This is especially useful for those on dial-up where the connection may take 30 to 45 seconds or more. Multiple transactions may be processed within the same connection, and IPOS will automatically detect and retry upon connection error.
- At the Server, ADR Server will monitoring total number of connections, and leave minimum of 10% room ready for new connections. In case there is to many IPOS "line-camping" occurrences reaching the tolerance ratio, ADR Server will drop those "idled" connections to free up serving resources.
- Multiple IPOS devices may reside within the same retailer location, sharing the same dedicated communication. In case of dial-up connection, one of the IPOS will be configured as the network "hub" to "route" remaining IPOS communications. In case some ISP's do not allow multiple shared access, each IPOS device will require separate dial-up lines. As an alternative, a "concentrator" router may be installed, in which case the IPOS modem and connection control will be disabled and relies on the "concentrator".
- For high-speed dedicated connections, the IPOS connection may share with retailer's existing phone-line because communication between IPOS and Merchant Server is encrypted and processed under independent channels and "sessions". For dial-up, the connection for ITE has to be dedicated, although the IPOS "hub" can "route" non-ITE transmissions, it is not recommended.
- Normally, for dial-up connections, each IPOS will be configured to make connection through their existing ISP (which is widely available). ADR Server will host a separate ISP at roughly a 10 to 1 ratio, as failsafe backup.

There are various other "messaging" protocols that IPOS will periodically, or upon server request, engage, handle and process.

3. The Cashier and the Customer

Cashier engages initial card swiping and product entry, and all the remaining validation process is strictly between the individual and the Server via the device. In case of any rejection or partial rejection occurs, it will be the individual's decision to accept or void. If they accept, they must obtain a receipt for manual claim if they wish to apply for the eligible rebate. This same rule applies to integrated POS systems. Rather than using IPOS, they will operate on their POS software, and the IPOS driver for actual machine validation will handle the claim.

Majority of Cashiers' task is their POS operation. In Relation to the ITE process:

- Swipe or scan the I.D. card, and enter or scan products
- Act according to the device's prompt
- Explain to and educate customers on the validation and rejection rules
- Only if applicable (if cards are issued and distributed at retailer) issue or replace cards

The customer will interact with and engage the validation process in real-time with the server via the device:

- Provide valid I.D. card to the cashier
- Enter validation criteria or Pin Number
- Occasionally, ask cashier for help or explanations for validation, rejections, card replacement etc.
- Occasionally, call and question the Government of his/her limits and rejections, possibly obtain the rejection receipt and file for manual claim

4. The Retailer

Retailers will get their daily tax exemption report, as well optionally retrieve totals and details of historic ITE claim rebates. Any action that needs to be taken by the retailer, IPOS will prompt the retailer within the IPOS message screen, and if it is critical or mandatory IPOS will be "annoying" within every ITE transaction. This provides an effective way of taking retailer's responsibility and accountability for their required actions like communication, firmware upgrade, and so on

The most common routine tasks carried by the retailers are:

- Sale and Return transactions for ITE claims
- Issue new or replacement cards (only if applicable)
- ITE Batch total and details.
- Respond to occasional or periodical server posted messages
- Entertain and educate customers on various validations and rejections
- Contact Wiz-Tec for technical or operational support

Rebate payment of the batch total amount will be guaranteed by the Government, unless the Government has sufficient evidence indicating retailer abuse or default

5. Other common functions

Other than a normal ITE transaction workflow, there are many other common procedures, including return/refund, card issuing, card replacement, batch total review, batch settlement, history total review, history detail review, server messaging (several), eligible product download, tax rate download, device validation download, firmware download, etc. Inside the Application Server, in addition to Process Server, there are various of dedicate server services provided within.

All data and message transmissions are securely encrypted via SSL, AES or VPN, handled by ADR communication Server. There are at least 2 identical servers running on the same physical machine, each capable of handling 100 or more simultaneously processes. In addition a separate set of database oriented Application Servers that hosts and processes government administrative operations. The actual server will be configured at no less than twice the IPOS devices deployed, since each IPOS may issue multiple simultaneous connections before failed connection is successfully dropped.

6. Automation, failsafe and external interface

Inside Merchant Server, there are Management Server and Automation Server, which are designed to specifically address common server oriented tasks. There are about 3 dozen scheduled tasks within to achieve fully automated server self maintenance, merchant batch settlement, merchant rebate submission, reporting, error recovery, error reporting, local database backup, failsafe database replication, external backup and so on.

7. The Government

Government accesses and achieves administrative operations using MSClient, over secured network tunnel (VPN or SSL) to dedicated Application Servers hosted within Merchant Server

The most common routine tasks carried by the Government are:

- Entertain individual inquiries for limit adjustment and occasional manual claims
- Administer card database for new or deactivated Indians, adjusting limits and validation rules
- Process weekly retailer rebates, submitted by Merchant Server
- Optional to exam and validate transactions and reports
- Occasionally administer or adjustment of eligible products and tax rate
- Contact Wiz-Tec for operational or technical support

8. Wiz-Tec

Wiz-Tec is responsible for running and maintaining the entire Merchant Server ITE program. The primary access from Wiz-Tec will be via remote control over secured network tunnel (VPN or SSL), on MSConsole and DBA tools hosted within Merchant Server

The tasks are divided into several areas (detail of each area will not be described here)

- System Maintenance: monitor and maintain the live Merchant Servers
- Development Services: interface, automate, update, test, fix of Merchant Server and IPOS

- DBA services: for database monitoring maintenance
- Technical and operational services: provided to both the government and retailers
- Communication services: troubleshoot and coordinate local communication providers
- Installation, setup, replacement and repair services: for retailers on IPOS devices
- Certification Services: services for 3rd party POS software integration