



SOVERAIN

233 S. Wacker Drive, Suite 9425, Chicago, IL 60606
www.Soverain.com

Transact Technology Guide

November 2009



Table of Contents

Introduction	3
Architecture	4
Application Configuration.....	4
Hardware Configuration.....	5
Production System	5
Firewalls	6
Transaction Database	6
Payment Gateways	7
Payment Mechanisms	7
Key Payment Features	7
3-D Secure	7
Payment Emulators	8
Payment Brands Spawning	8
Certified Payment Gateway Specifications	8
Commerce Objects	9
Securelink Technology.....	10
Next Steps	11

Introduction

Selling online today is more of a challenge than ever, with increasing security concerns and the critical need for trouble-free processing (see Figure 1. *What is Internet Commerce?*). Soverain's customers trust Transact - a robust e-commerce system with a decade of reliable, secure performance – for their online businesses.

Transact works with a broad array of e-businesses and supports multiple business models, payment methods, and currencies. Transact handles the complexities of Internet commerce, allowing organizations to concentrate on building an effective, successful e-business strategy.

What is Internet Commerce?	
Business	Marketing/Sales
Processing Orders	Analyzing Opportunities
Processing Payment	Attracting Buyers
Addressing Fulfillment	Personalizing Services
Providing Self-service	Helping Buyers Search
Providing Customer Service	Promoting Products
Analyzing Results	Recording the Order

Figure 1. What is Internet Commerce?

Transact was originally developed by incorporating e-commerce industry best practices into a standard application. Rather than having to develop an infrastructure from an e-commerce toolkit, offering or bundle, Transact customers benefit from a full-featured, time-tested e-commerce system. This cuts down on unnecessary consulting requirements, which reduces the risk, cost and time of a Transact implementation.

Transact uses common technologies to ensure security in an open network environment - including public key cryptography, secret key cryptography, 3-D Secure, authentication, authorization, and certificates of identity. Transact uses several subsystems, related through internal and external APIs, and a database. Transact 7 runs on Sun One Web Server 6.1 SP1 (formerly Netscape Enterprise Server), and uses other software servers as necessary within the Transact subsystems.

This technology guide provides a brief introduction to significant Transact components including:

- Transact Architecture
- Payment Gateways
- Commerce Objects
- Securelink Technology

Additional detail on these topics and others – including installation, administration, and security among others – is included in the Transact documentation set available via the Transact Technical Support Center.

Architecture

Transact's distributed architecture (see Figure 2. *Transact Architecture*) can support multiple merchant configurations. One Transact installation enables merchants to have multiple stores and companies with multiple business units to leverage one common infrastructure.

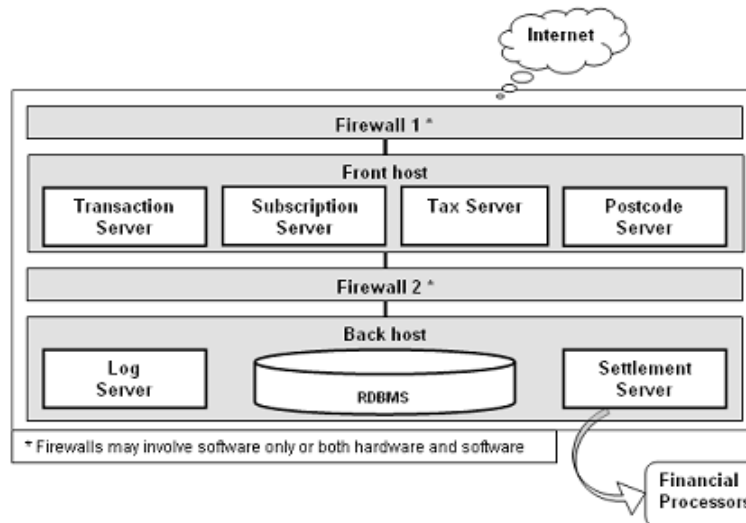


Figure 2. Transact Architecture

Application Configuration

A base Transact installation requires three servers:

- A transaction server that includes subsystems that process validation, authentication, authorization, operations, tax, and postcode data.
- A settlement server that communicates with payment processors to ensure settlement of purchases and the transfer of funds from the buyer to the seller's acquirer.
- A log server that manages all log entries generated by the Transact servers.

Optionally, depending on their requirements, customers can install a subscription server to manage subscriptions and authorize access to digital content.

Transact is hosted by Sun Java System Web Server 6.1, the Sun-Netscape alliance high performance Web server for e-commerce. For Transact, Sun Java System Web Server consists of three separate servers, each running on a separate port:

- An administration server that provides a forms-based interface for configuring and managing the following two servers.
- A HTTP server that handles all non-secure HTTP requests.
- A SSL server that handles all secure SSL requests.

Additional functionality required by Transact is provided through a set of Web server extension modules, or plugins, which are installed as part of the Transact installation procedure and loaded by the Sun Java System Web Server on initialization.

These extensions provide the following features:

- Ticketing-based access management (digital ticket and digital receipt access control) provides a powerful way to protect content using Transact's ticketing technology. Special ticketing directives can be placed within regions to require a valid ticket for access to content.
- Regional processing provides a way to divide the server's content into many individual regions, and enables the implementation of customized access control rules for each region. For example, the Transact CGI password mechanism can be used to protect content using basic authentication by a CGI script.
- FastCGI provides a high-performance alternative to CGI by keeping application processes running between requests. FastCGI eliminates the CGI overhead – the overhead of starting a new process and initializing an application (for example, connecting to a database) each time somebody requests a document.

The Transact Web server extension modules are incorporated using the Netscape Server Application Programming Interface (NSAPI).

Hardware Configuration

Soverain recommends that customers install two separate Transact systems:

- A production, or live, Transact system
- A development, or testing, Transact system

Production System

Soverain recommends that customers install the production system on two host machines, a front host and a back host. Customers must make sure that they have sufficient access control to ensure the physical security of both machines.

Front Host Server

The Sun Java System Web Server, the transaction server, and, if applicable, the subscription server are installed on the front host machine. The front host is connected to the Internet and serves HTML and CGI applications to buyers and sellers via HTTP and Secure Sockets Layers (SSL). The standard port numbers are 80 for the HTTP server and 443 for the SSL server; however, administrators can assign any port numbers they choose.

The transaction and subscription servers are located on the front host machine making them directly accessible to any buyer on the Internet. Tax data and postcode data are periodically updated with current tax rules and postal codes on the front host by the transaction server. The tax scripts are also used by sellers and online businesses during store registration.

Back Host Server

The Sun Java System Web Server, as well as the settlement server and the log server, are installed on the back host machine. The back host is not connected directly to the Internet. A firewall resides between the front and back host ensuring protection of the secure information on the back host machine from any Internet-based attack.

The database must also reside on the back host because it contains sensitive account information, such as payment card numbers and other buyer and seller information. The local area network (LAN) connecting the front and back host machines must also be secure and isolated from any public networks. The secure LAN must connect only the Transact host machines.

Each server on the back host requires some type of security protection:

- The database is protected because it includes sensitive customer data.
- The settlement server is protected from attackers issuing fraudulent charges or credits through a payment agent.
- The log server records valuable information that is protected from attacks.

Firewalls

Soverain recommends the installation of two firewalls:

- One between the front host and the Internet
- One between the front host and back host

The front host machine communicates with the back host through ports for HTTP and HTTPS, the log server, and the database. This means the firewall has to be configured to allow traffic addressed to one or more of its aliases on all four ports to be sent to the back host on its relevant ports.

The back host machine allows access to itself not from the front machine but from the firewall. The back host might have an entirely different domain name from the front host, if it has a domain name at all.

Transaction Database

The transaction database is a relational database that stores all buyer, merchant, administrator, and transaction information. Transact supports use Oracle® relational database managers.

Due to the nature of online transaction processing, Transact is not a single, simple, linear application. It consists of a number of CGI scripts attached to a Web server. The functions for taking orders, registering customers, reporting store activities, and so on, are each performed by a separate module. Some functions are triggered by a demand, such as a buyer making a purchase. Others are run on a regular schedule. Each function reads information from the database and leaves its results in the database.

As a result, the Transact database is the central hub providing communication among all the different functions that, as a whole, comprise Transact. It is critical to the proper operation of Transact and was designed for maximum efficiency in performing these tasks.

Payment Gateways

The Transact payment subsystem handles Transact's monetary transactions. The subsystem manages account information, handles payment authorization, manages the actual transfer of money, and maintains a log of all monetary activities.

Transact has established business relationships with payment processors with whom Transact customers do business. A payment processor is a company that performs authorization and settlement of payment card payments. Sellers who sell their products to cardholders over the Internet retain the services of one or more processors who handle payment cards that the seller accepts.

Payment Mechanisms

Transact supports all types of payment mechanisms, including:

- Purchase orders
- Credit cards
- Procurement cards
- Microtransactions
- Debit cards
- Smart cards
- Frequent-buyer points

Key Payment Features

Transact performs real-time authorization requests and automatic settlement. It supports automatic subscription renewals and partial billing and credits with payment reauthorization. It also manages state sales taxes and VAT, including distance-selling thresholds. Multiple currencies and payment methods are provided with built-in support for First USA/PaymentTech, First Data Corp and ISO 8583 for international payment processing.

3-D Secure

Visa's Verified by Visa and MasterCard's SecureCode are based on the 3-D Secure protocol, a recent payment security initiative. Developed by Visa to improve the security of Internet payments, 3-D Secure is designed to allow the authentication of card holders by their issuers at participating merchants. Designed to add a new level of security to e-commerce, 3-D Secure verifies the card holder's identity using a password as well as addresses charge-backs which impact online merchants frequently. Real-time authentication of card holders can dramatically reduce costly fraud and chargeback processing.

3-D Secure aims to shift the internet card-not-present environment to the more secure card-present environment, which is typical of today's stores that require a card to process a transaction. The digitally signed receipt provides a merchant with evidence of a card holder's approval of a transaction. The Visa International Operating Regulations specify that Issuers may not charge back electronic commerce transactions if the transaction involved a 3-D Secure authentication or attempted authentication.

Transact provides 3-D Secure functionality using third-party Merchant Plug-in software. The current version of Transact supports Arcot TransFort MPI Ver.5.7.0.

Payment Emulators

Transact provides payment gateway emulators to enable quicker functionality deployment, simulating the Paymentech, FDC or ISO 8583 protocol acquirers request and response mechanism. Transact also has 3-D Secure MPI and ACS simulators for testing the 3-D Secure configuration prior to a merchant attempting Visa PIT or MasterCard Valfac 3-D Secure compliance certification testing.

Payment Brands Spawning

Transact supports spawning of new payment brands with configurable credit card number lengths and bank identification numbers in addition to the default Visa or MasterCard brands.

Certified Payment Gateway Specifications

Recently certified payment gateway specifications include:

- Paymentech Online Payment Processing Rev 7.0 including
 - Online authorization -- mandatory authorization data, full billing address for address verification, Card Security Value (CVV2/CVC2/CID)
 - Batch settlement -- mandatory settlement data
- First Data Corporation (FDC) Version 8.2 including:
 - Online authorization -- mandatory authorization data, address verification auxiliary data, e-commerce request message data, card code data (CVV2/CVC2/CID)
 - Batch settlement -- mandatory settlement data, e-commerce request message data, customer presence ID, card presence ID, authorization response data for card code (CVV2/CVC2/CID)

Commerce Objects

All e-commerce systems handle the authentication, order, monetary exchange, verification, and fulfillment. What sets Transact apart is the use of Transact Commerce Objects.

For a Web site to benefit from commerce services provided by a centralized services site, the two sites must be able to communicate information back and forth securely. Commerce Objects are a technique for transmitting authenticated data across the Web. They rely on Uniform Resource Locators (URLs), a standard feature of the HTTP protocol. Because this method of authenticated communication uses standard URLs, it requires neither dedicated connections between participants nor special new protocols. It also provides universal browser support, since it does not require any special software (applets or plug-ins) on the client side other than the browser.

A Commerce Object:

- Identifies its intended recipient. For example, a Commerce Object may be created by a store owner and be intended to be received by a CSP. A buyer's decision to buy activates the Commerce Object, but the intended recipient in this sense is still the CSP.
- Transmits a short stream of data -- approximately 8,000 bytes or less, in most cases.
- Provides the recipient with the means to ascertain whether the data was created by a known, authorized party.
- Provides the recipient with the means to detect whether data was modified since the time it was created, either through malicious tampering or accidental data corruption.

Transact has implemented a variety of Commerce Objects to address the various stages in the Internet commerce cycle:

- Digital offers
- Digital receipts
- Digital coupons
- Digital queries
- Digital tickets

Securelink Technology

Soverain's SecureLink technology allows customers to commerce-enable any site, anywhere on the Internet by dropping offers and "buy" buttons that link to the robust order management system. Unique SecureLink Commerce Objects allow for distributed commerce, providing tamperproof messages and authentication. Transact keeps sensitive information behind not one, but two firewalls. All customer payment credentials are independently encrypted.

Transact supports the separation of content management from order processing and customer service for optimal security, scalability, and manageability. The SecureLink API enables support for multiple content servers in multiple locations for multiple businesses. This means Transact can serve more buyers than other systems that lack a distributed architecture.

The SecureLink Bridge protects information on non-Soverain Software Web servers, so that only users that have been authorized by a Transact system can access that information. The SecureLink Bridge works with Transact systems to protect digital goods and subscription information on fulfillment servers, so that only customers who have paid for the digital goods or subscriptions can access them. In addition, SecureLink can track and log user sessions so that a log analysis tool, such as Soverain Software WebReporter, can generate reports detailing user access patterns.

Other SecureLink Bridge features and functions include:

- Flexible encryption and authentication. SecureLink Bridge supports simultaneous use of HTTP, SSL, and PCT protocols, thus providing maximum flexibility in protecting the privacy and integrity of your server's interactions with clients. SecureLink Bridge implements both encryption and digital signatures.
 - Flexible access control. SecureLink Bridge can control access to the server on the basis of such factors as ticket, URL, hostname, time of day, username, browser type, version, and authentication method.
 - Custom applications. SecureLink provides powerful API's and Web Services to build custom applications using popular languages to manage stores, buyer accounts and order entry.
 - Enhanced logging facilities. SecureLink Bridge provides an enhanced log format that integrates each request's access, error, and security information. This enhanced format also provides fields for logging the browser type, the referring URL, and the request begin and end times. The format is designed to be extensible and easy to parse.
 - SecureLink Bridge supports the common access and error log format widely used by existing Web servers.
 - Enhanced support for X509 version 3.0 certificates, including full support for this latest version of the standard client authentication.
 - Support for client authentication in SSL and PCT. SecureLink Bridge can request or require a client to authenticate itself, and can restrict access based on client authentication information using region commands or CGI variables.
 - Forms-based administration tool. This feature allows the administration of most SecureLink Bridge operations through an HTTP forms-based interface.
 - Digest access authentication. This feature provides a challenge/response authentication mechanism that provides additional security -- the user's password is not sent over the network.
 - Safe restart. This feature allows administrators to restart SecureLink Bridge to implement a new configuration without having to drop existing client connections.
-

Next Steps

This Technology Guide provides a brief introduction to the Sovereign components used to create an e-commerce infrastructure:

- Hosting tasks, for example, enabling secure transaction processing on the server that hosts the Web store content.
- Web site development tasks, for example, implementing payment gateways to handle monetary transactions.
- Business tasks, for example, setting up relevant third-party business relationships.

For more information on the Transact distributed Internet commerce model, refer to the following documentation (available in both HTML and pdf format on the Transact Technical Support site):

- For background and overview information on Internet commerce in general, and on Transact in particular, refer to the *Getting Started* series of concept manuals.
- For a perspective of working with Transact from the sell side, consult the *Running a Web Store* series of manuals.
- Consult the *Installation Guide* for information on system requirements, Web server setup, and Transact installation and initial configuration.
- If upgrading from an earlier (5.x.x) release of Transact, refer to the *Upgrade Guide*.
- For information specific to using Smart Pages to customize the Transact experience, including how to set up for the international marketplace, refer to the *Customization Guide*.
- Information on setting up and using reporting facilities available with Transact can be found in the *Data Warehouse Reporting* series of manuals.
- Rounding out the documentation set is the *Database Schema Guide*, a complete reference to database tables and field definitions for Oracle; and, there is also extensive API documentation in the form of reference pages and programmer's guides with real-world examples, covering the gamut of programmatic interfaces to the system.