OmniCrypto
Product Description
V8.0
June 2, 2008

OmniCrypto is licensed software from Opsol Integrators Inc. and can be purchased as a stand-alone version or integrated with OmniHub. Contact Yash Kapadia at +1 408 446 9274 or email Yash@Opsol.com for more information.

1 Introduction

The OmniCrypto product suite provides customers with a complete and secure solution for businesses that process transactions on ATM, Point of Sale devices and other financial networks.

OmniCrypto uses Atalla hardware security and currently supports Atalla PCI cards, A10150, A10100 (Variant and AKB version), A10000E Security Processors, A7000 Security Processors and A4000 Security Processors. It communicates with multiple Hardware Security Modules to achieve fault tolerance and load balancing.

OmniCrypto is supported on the following platforms:

- HP NonStop Integrity and Blade servers,
- Windows servers

2 Product Families

Based on a modern, component-based design and an open, standards-based architecture, OmniCrypto product suite provides a secure solution - extending existing IT investment, while providing the highest levels of security and flexibility. The OmniCrypto product family consists of modules to support ATM/POS transaction security, ATM key management, Public Key Infrastructure (PKI), encryption and tamper-proofing of database/files, passwords and credentials based user authentication, role based Access Control Lists (ACL) for authorization of users and more.

2.1 OmniCrypto ATM Card and PIN Management

OmniCrypto provides PIN management solution fully compliant with all key management requirements as established by ANSI X9.8 (3DES) and ANSI X9.24 (Unique Keys). Processing PIN typically involves the following tasks –

- Generate PIN mailer
- Encrypting PIN or PIN block
- Translating PIN block
- Verifying incoming PIN block and authorizing or denying transaction requests.

OmniCrypto supports 3DES PIN encryption using double or triple length DES keys and following PIN block types:

- ANSI (format 0)
- IBM 3624
- PIN/pad character (Diebold)
- Docutel
- IBM encrypting PIN pad
- Burroughs
- IBM 4731
- Visa unique key per transaction

PIN must be translated as it travels through the system for verification at every intercepting processor/node. OmniCrypto can translate a PIN block to and from any of the above-mentioned PIN block types from incoming PIN encryption key to outgoing PIN encryption key OmniCrypto uses Atalla Hardware Security Module for PIN management. It supports following algorithms for PIN verification:

- Identikey
- IBM 3624

- Visa
- Atalla DES Bilevel
- Diebold
- NCR
- Burroughs
- Atalla 2x2

OmniCrypto supports following card verification methods:

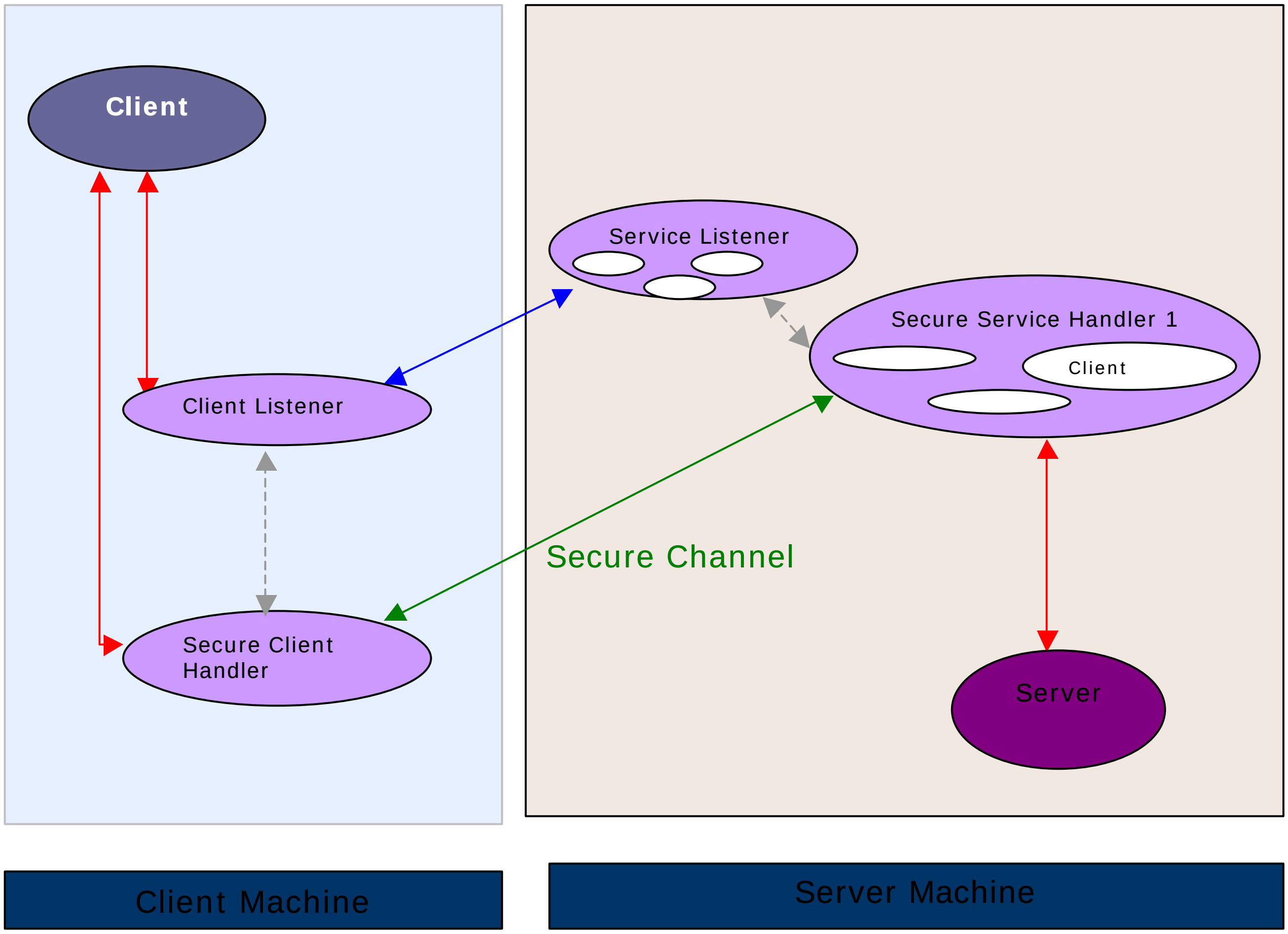
- Visa Card Verification Values (CVV, CVV2, iCVV)
- CHIP Card (ARQC)
- American Express Card Security Code (CSC)
- MasterCard Card Verification Code (CVC)

2.2 OmniCrypto SecureChannel

OmniCrypto SecureChannel allows client applications to communicate securely using secure socket layer (SSL) with server applications without any code change. OmniCrypto SecureChannel core adapters provide complete data encryption and authentication using X509 digital certificates/signatures between clients and servers using it. Add-on adapters allow it to be used with specific middleware applications like Tuxedo, Pathway servers and web services (SOAP).

Server side adapters run on NonStop platform. Client side adapters can run on Windows, NonStop and Unix/Linux platforms. It is designed to scale well with load to perform optimally under high transaction load when multiple clients are connected and sending requests.

Architecture Diagram



Features

- Scalable

  As shown in the architecture diagram, listener adapter starts and monitors the secure service handler processes. Each handler process is multi-threaded and can support multiple connections at a time. Attributes like CPU, number of threads and priority can be specified for handler processes for optimal load-balancing. For even more scalability, multiple listener adapters having its own set of handler processes can be started.

- Transparent to applications

  No code change required by current client/server applications to use SSL secured channel for sending transaction data

- Allows for gradual migration of clients to use secure channel

  Secure and non-secure channels co-exist in this architecture. This allows clients to be migrated to use secure channel gradually without disrupting/affecting non-secure client processing.

- Allows clients to switchover between secure and non-secure channel by simply updating client configuration to point to client listener or application server.

- Flexible

  Configuration allows specifying number of secure service handlers to run and how to start/stop them. Secure service handlers can be started when service listener adapter starts or when a client request comes in and a new Secure service is needed to handle the load. A mix of both types of service listeners is also allowed for even more flexibility. Also, secure service handlers can be configured to stop themselves after an inactivity timeout. It is also possible to configure secure service handlers to run independently once started by service listener. This can be useful when secure service handlers needs to be stopped/restarted without affecting the current clients already connected and sending transactions over secure channel.

- Extensible

  More optional add-on adapters can be added to the existing set of adapters for even more functionality. For example, secure-logging adapters can log all or selective transaction data to a data store in encrypted form. Secure service handler acts as a single point of entry into the system and all secured transaction data pass through it. This makes it a logical choice for performing transaction logging and other functions like data transformations, and even forking the transaction to another application and consolidating the result back into a single response with enriched/added information.

- Server Load Distribution

  Its flexible and modular architecture allows it to run on a separate machine other than the machine running your existing server. Also, it can spread the processing of the encryption and decryption currently done by a secure application to another dedicated machine, effectively increasing the performance of existing secure servers.

2.3 OmniCrypto Data at Rest Encryption

Data at Rest encryption secures confidential data stored on networked servers from attackers who already have or can easily gain access to the data. Encryption of the sensitive data can provide strong security, but it needs development of an encryption strategy taking many factors into consideration such as encryption key management, access control and authentication, defining sensitive data and performing encryption. This document describes Opsol's Data at Rest Encryption product that solves this problem in compliance with industry standards like Payment Card Industry (PCI) Data Security, Health Insurance Portability and Accountability (HIPPA), Gramm-Leach-Billey-Act (GLBA) and many more.

Architecture Diagram

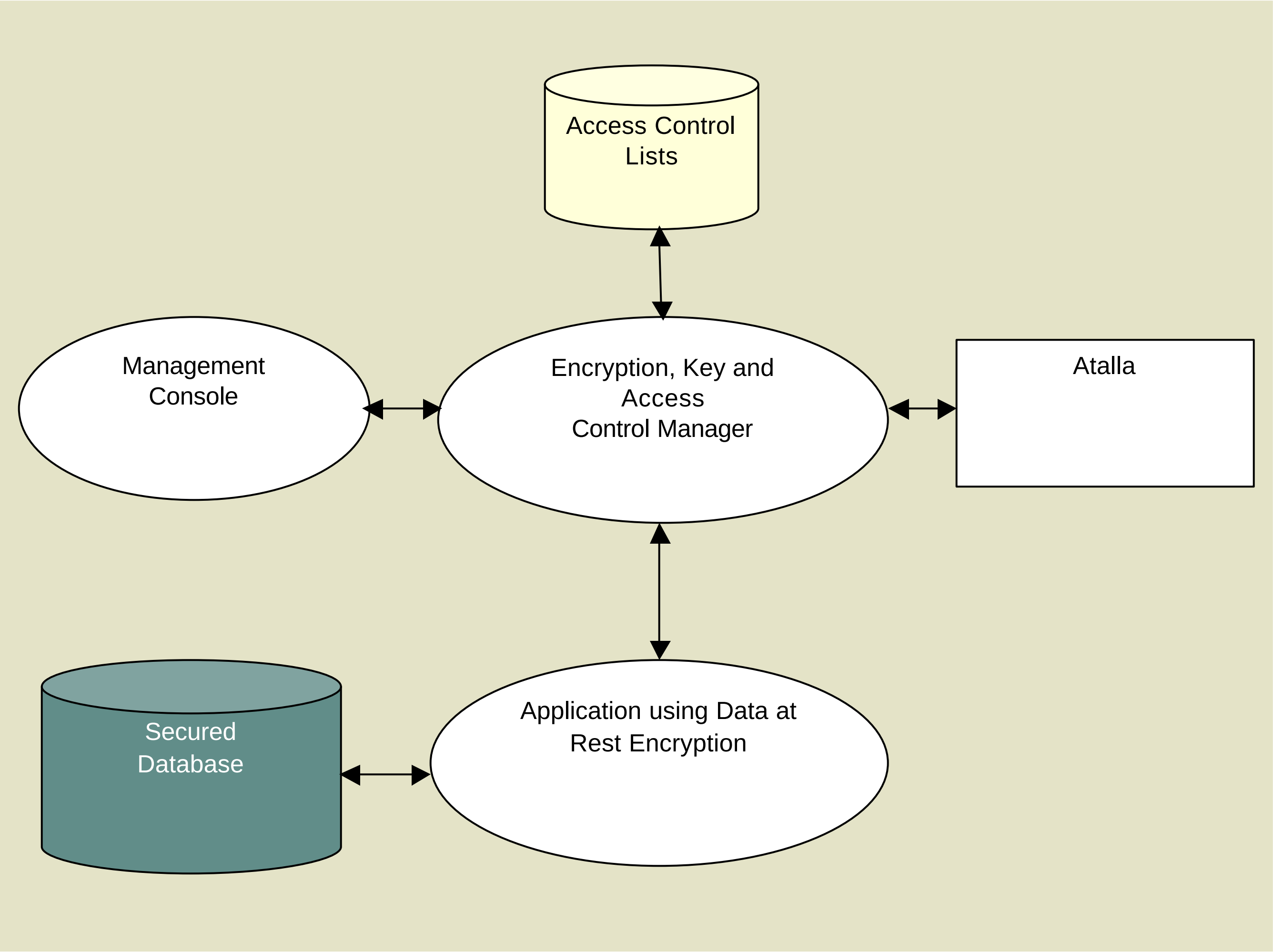

Access Control Lists
Management Console
Encryption, Key and Access Control Manager
Atalla
Secured Database
Application using Data at Rest Encryption

Figure 1. Data at Rest Encryption Architecture

Features

- Provides secure key management using tamper-proof Atalla hardware and security techniques like dual custody of keys.
- Allows changing the encryption key frequently without any downtime.
- Provides selective encryption of data to secure the sensitive data in the database. Access control lists decide who can access a sensitive field.
- Also provides bulk encryption of the complete database so that data can be stored for archival or transported to another location securely.
- Comes with an easy to use Graphical User Interface to manage data, keys, access control lists and application authentication.
- Provides detailed audit logs of activity.
- Supports application migration to use Data at Rest Encryption with no down time.
- Supports mySQL, Oracle, and NonStop SQL databases.

2.4 OmniCrypto Key Management

2.4.1 Management of Unique and Dynamic keys per ATM/POS (ANSI X9.24)

OmniCrypto provides a complete solution to generate and remotely load unique keys (ATM-A, ATM-B/Communication key, PIN key) in ATM/POS devices as per ANSI X9.24. Solution is easily implemented and complies with ANSI standards and network operating rules. OmniCrypto also supports manual unique key loading to older ATMs that will never be upgraded to allow remote key loading.

Remote Key Loading

OmniCrypto uses industry standard RSA cryptosystem to implement digital certificate based solution for remote key loading. ATMs with support for RSA cryptosystem but without any preinstalled private key/digital certificates by manufacturer can also be injected remotely with unique key. OmniCrypto creates a SSL like session to ATM key loader, generates keys to be injected and securely inject the DES keys into ATM. It also integrates with existing host database to export the new keys there. This makes the process completely automated and ATM immediately ready for sending the test transaction with unique keys.

Manual Key Loading

For older ATMs, that do not support RSA cryptosystem and will never be upgraded, OmniCrypto provides a semi-automated solution to unique key mandate. OmniCrypto generates unique key in number of components that must be put into ATM separately as per the ANSI standard. To make the process secure, OmniCrypto provides role and permissions based access to different operations in the process. There are few predefined user roles that can be further modified to fine tune the access control. OmniCrypto Security Officer (OSO) maintains users. OmniCrypto Security Manager manages user roles and permissions. Key Generator User (KGU) generates the unique keys for an ATM (or ATMs in batch mode). OmniCrypto prints the key components in secure envelopes

(PIN mailers). These secure envelopes are sent to the branch to be distributed to Key Loader Users. OmniCrypto verifies that same user loads no two components in the same ATM. On successful loading of components in the ATM, OmniCrypto generates the final unique ATM key in the same way it is created inside the ATM, and updates the host database with new key. ATM can then be tested with a test transaction.

2.4.2 Key exchanges, secure key transport across hosts

OmniCrypto uses industry leading Hardware Security Modules to support Key Exchanges between financial institutions and switches. It also provides a completely secure channel to exchange sensitive information between two nodes. It combines PKI with symmetric keys to create a secure channel without the need to have a pre-arranged symmetric key sharing.

2.4.3 Secure key storage

OmniCrypto uses Hardware Security Modules to provide secure key storage. Using HSMs guarantees that no key will ever be present in clear outside the security module and increases the security of the whole system multifold.

2.5 Digital Certificates, Signatures, Secure Email (SMIME)

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet. PKI integrate digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

PKI protects your information assets in several essential ways:

- Authenticate identity
- Verify integrity
- Ensure privacy
- Authorize access
- Support for nonrepudiation

OmniCrypto supports generating RSA key pairs, X509 v3 Digital Certificates (PEM/DER), and verifying the contents of a X509 Digital Certificate. Combined with its user authentication and authorization component, OmniCrypto provides a complete solution to implement PKI in an organization. OmniCrypto supports following functions typically required for implementing a PKI solution:

- X.509v3 Digital Certificates - Generation, Verification, Import/Export.
- Digital Signatures – Digitally signing data, Verifying digital signature on data.
- RSA Public-Private key pairs – Generation, Import/Export to/from Digital Certificates.
- Data envelopes containing 3DES keys and encrypted data – Import, Export, Create, Receive and Verify Data envelopes

- SMIME – By using Digital Certificates, Digital Signatures and Data envelopes, OmniCrypto can add SMIME support to any email server.

2.6 HSM device and key management

OmniCrypto can work with multiple Atalla NSP devices. It can manage multiple HSM devices by grouping same type of devices into pools. Depending on the type of transaction, it selects the pool of devices to use. With in a pool, it performs load-balancing to ensure optimal use of all Atalla devices. It also supports grouping of HSMs with in a pool based on master file key loaded in the devices. It provides web-based console for management of HSM devices and keys. Each device and key in the system has a unique id. Applications using OmniCrypto for HSM device and key management can direct transactions to a particular HSM or delegate the responsibility to OmniCrypto to use the proper device from the pool for optimal performance.

Following device management functions are supported through web-based console:

- Add device (add a device to the system)
- Delete device (permanently deletes device from the system)
- Service device (temporarily brings HSM to service mode from production mode)
- Update device (change device configuration)
- Query device (status/statistics)

Following key management functions are also supported through web-based console:

- Load key
- Delete key
- Verify key
- Change key

Most of these operations can be done online without affecting any transactions. OmniCrypto internally performs the load-balancing and divert the traffic to alternate device while one HSM is being updated or serviced.

2.7 User Management with Role Based Access Control

Provides a complete solution for role and permissions based user authentication and authorization. User authentication and permissions specify who is allowed to use the system, what credentials they have to present, what actions they can take, and what data they are allowed to view and manipulate.

After OmniCrypto checks the user’s credentials, it determines what the user should be allowed to do, based on a number of factors. Access policies can be defined broadly on the basis of user roles or narrowly based on the IP address of the user (Host Access), user’s permissions within a role to which the user belongs. Through these mechanisms, user access can be restricted in several dimensions, including:

- Restricting the client IP address
- Restricting the access to the system based on role and permissions assigned
- Grouping users into roles
- Restricting which actions may be performed under each role.
- Restricting user access to within certain days/times

OmniCrypto provides a very generic solution that can be easily customized to suit the need of customer. Customer first needs to define all the operations that need to be monitored and controlled via OmniCrypto system. Next step is to define user roles based on the operations each role can perform. Same operation can belong to multiple roles, making it extremely flexible. Last step is to add the user and assign a role and if finer control is needed, adjust the user permissions from the superset of operations defined for the role. OmniCrypto comes with few predefined user roles and operations to perform user management operations (ADD/VIEW/DELETE/MODIFY users) and report generation (AUDIT/REPORT).

OmniCrypto also supports up to 16 more credentials. It allows defining the various combinations of credentials that can be used to authenticate and authorize the user. On a successful authentication, it generates and returns a secure session key that can be used to maintain and authorize the session. All credentials and sensitive information is stored securely in the database. User session management is fully customizable, allowing different inactivity timeouts for users, number of concurrent sessions per user and blocking a session after a number of unsuccessful logon attempts.