

Credit Card Encryption in SAP Environments

Ingrian and Princeton Payment Enable Seamless Encryption in SAP R/3

Executive Summary

Encryption has become a clear mandate for any organization that collects or processes payment data. Yet making encryption work within an enterprise has traditionally been a challenge, particularly for large organizations with SAP applications. Today, these organizations can leverage a combined solution from Ingrian® and Princeton Payment Solutions that makes it easy to gain the security benefits of encryption, while minimizing its costs and business impact.

Today, retail merchants, payment processors, and financial institutions, must guard against data thefts and validate compliance with credit card association security guidelines such as the Payment Card Industry (PCI) Data Security Standard. To do so, these companies need to encrypt credit card data in applications and databases. Yet addressing this mandate is proving to be a significant challenge for many organizations, particularly those with SAP environments.

While SAP R/3 provides encryption libraries, these libraries present performance and key management limitations that make them impractical for most organizations to deploy. Ingrian Networks and Princeton Payment Solutions bring high-performance, tightly integrated cryptographic capabilities to SAP applications. With their combined solution, the companies enable organizations with SAP applications to encrypt and fully secure their credit card data—and to do so with unmatched efficiency and performance.

The Ingrian DataSecure® Platform is the only appliance-based encryption solution available today that combines granular, field-level encryption capabilities and the flexibility to integrate at the Web server, application server, or database layer. Princeton Payment Solutions' CardSecure® application is a software-based solution that brings tightly integrated encryption

capabilities to SAP environments. By harnessing the combination of CardSecure's tight integration with SAP and DataSecure's dedicated hardware appliance, organizations gain a range of benefits:

- **Sophisticated key management** capabilities, offering security managers and system administrators a range of benefits, for example, the ability to perform ongoing key rotation without incurring any SAP downtime.
- **Robust security**, offering strong access and authorization capabilities, centralized key storage and management, secure data transfer, and more.
- **Streamlined implementation**, with centralized administration and policy management, capabilities for automating the conversion of unencrypted data, and seamless SAP integration.
- **High performance** and reliability, with all cryptographic processing taking place on the Ingrian appliance—offloading all processing from the SAP platform, and minimizing the business impact of encryption.

Sophisticated Key Management

While encryption can help prevent data theft, ultimately your data is only as safe as the keys that protect it. To efficiently protect against the

myriad threats confronting enterprises today, cryptographic keys need to be secured, and centrally managed.

With the combined solution of CardSecure and DataSecure, organizations gain sophisticated control over their cryptographic keys. CardSecure's innovative key management capabilities allow administrators to do key rotation without taking the SAP application off line. Further, this key rotation happens independently of the SAP R/3 systems. In this way, organizations can avoid the severe performance penalties and administrative complexity associated with using SAP's encryption libraries.

With this combined solution, cryptographic keys and authorization policies always reside on Ingrian's hardened appliance. This significantly simplifies management of key backup, restoration, and key rotation since all keys are stored in one place.

Robust Security

Ingrian and Princeton Payment Solutions enable organizations to encrypt credit card data in SAP environments, and they offer a range of features that maximize the security of sensitive cardholder data. CardSecure and DataSecure offer support for 3DES, a strong, standards-based cryptographic algorithm, and the transmission of data between the SAP environment, the CardSecure platform, and the Ingrian appliance can be secured via SSL.

As mentioned above, by using the CardSecure and DataSecure solution, cryptographic keys always reside on the DataSecure appliance. Simply by minimizing the number

of locations in which cryptographic keys reside, organizations can help minimize the danger of keys being compromised. But DataSecure offers a number of features that ensure keys are safe on the appliance. For example, when an encryption key is "at rest" on the internal DataSecure disk, it is twice-encrypted for added security using several internal Ingrian keys designed for this purpose.

Further, the DataSecure appliance is hardened for security. For example, the appliance has no "back door" access, limited open ports, network-based listening protocols can't access keys, and configuration files are encrypted. For added security, the platform can be configured so that individual administrators are granted access only to areas for which they are responsible. DataSecure offers over 20 access control lists (ACLs), which offer granular control over administrative functions. For example, one administrator might only be given access to network configuration functions, while another might only be given access to certificate management controls. This level of granular access control enables customers to control and closely monitor administration operations.

In addition, DataSecure platforms offer these security features:

- Secure, multi-factor authentication and access control between the DataSecure platform and the servers and databases accessing the platform.
- Granular authorization capabilities that enable constraints to be placed on user operations based on specific key permissions.
- Active alerting capabilities so that, if attempts to breach

protected data occur, mechanisms are employed to alert administrators.

- Comprehensive, secure, and centralized logging and auditing of all cryptographic functions and access.

Streamlined Implementation

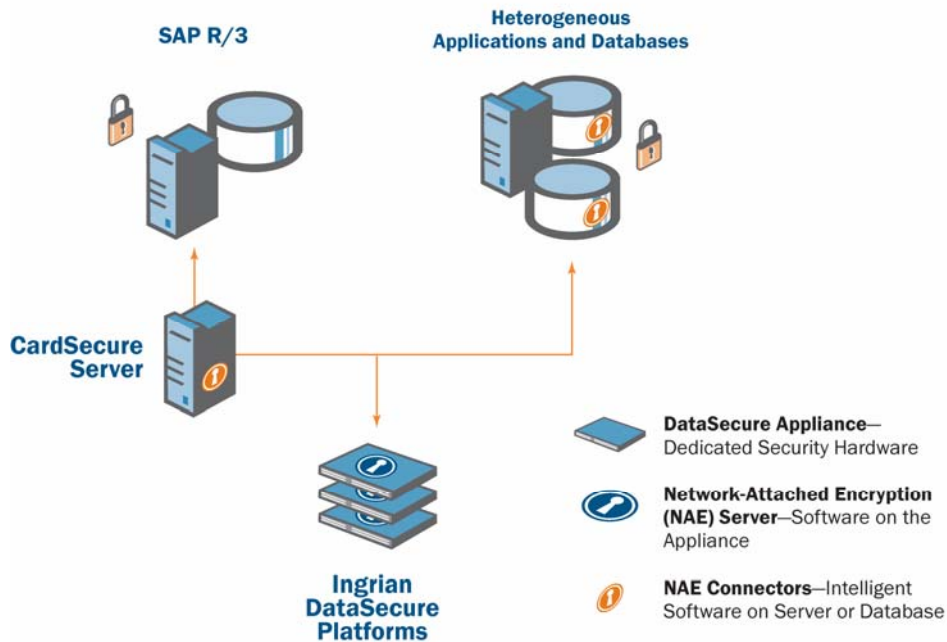
With the combination of DataSecure platforms and CardSecure products, organizations can quickly and efficiently start encrypting credit card data in SAP R/3 systems.

With CardSecure, SAP applications need only be revised to make a standard remote function call (RFC) to the CardSecure server, which will then receive all cryptographic requests directly from SAP. CardSecure has the intelligence to work with native credit card number fields within SAP, ensuring proper handling of encryption and decryption requests. Upon initial deployment, CardSecure will also automatically migrate existing credit card numbers from plain text into an encrypted format—without any application downtime.

The DataSecure platform can be efficiently integrated with CardSecure products, enabling organizations to quickly harness the key management and cryptographic processing capabilities of the DataSecure solution. Further, the DataSecure platform helps streamline ongoing administration. This is achieved through the following:

- Easy-to-use, intuitive management via a graphical user interface.
- Centralized management of all policies, users, and cryptographic keys.
- Automated replication between Ingrian products.

Enterprise Deployment Architecture



CardSecure integrates seamlessly with SAP R/3, receiving all encryption and decryption requests from the SAP server via standard RFC commands. DataSecure appliances handle all key storage and cryptographic processing, and can also be integrated directly with the organization's database, as well as other application servers and Web servers.

High Performance and Reliability

With the combined solution, all cryptographic processing is centralized on the DataSecure appliance, a highly specialized appliance that delivers high performance and convenient scalability. The solution can process 30-40 transactions per second, and Ingrian makes it easy, through load balancing capabilities, to add additional appliances and boost scalability as performance needs dictate. Further, with CardSecure's online migration capabilities, credit card numbers can be converted from plain text to encrypted format, while all associated applications remain online—minimizing the impact of encryption on the business.

By offloading CPU-intensive cryptographic processing from disparate servers and databases, DataSecure restores server and database performance to optimal levels—resulting in less waiting for information and higher resource utilization.

In addition, DataSecure offers an array of features to ensure reliability and availability:

- High availability. Featuring redundant power supplies, fans, and processors on each appliance, DataSecure also enables the use of redundant, replicated appliances and failover configurations that ensure optimal up time.
- Health checking. Web servers, application servers, and databases can determine immediately if an appliance is unavailable and switch to an alternate.

With its broad deployment capabilities, DataSecure streamlines the implementation of encryption throughout an enterprise, even in heterogeneous environments. DataSecure platforms can function as the central cryptographic engine for all enterprise encryption—a single appliance can support the encryption and decryption requirements of a number of disparate servers and applications.

In addition to support for SAP environments, which is enabled through CardSecure, DataSecure platforms can be integrated directly with a range of systems:

- All application servers, including those from BEA, IBM, Microsoft, Oracle, and Sun.
- IBM DB2; Microsoft SQL Server; and Oracle 8i, 9i, and 10g databases.
- PeopleSoft applications, including Human Capital Management, Customer Relationship Management, and Financial applications.
- All Web servers, including Apache, Tomcat, Resin, and Microsoft IIS.
- Legacy and custom environments via an XML, JCE, MS-CAPI, .Net, or PKCS#11 interface.

- Disaster recovery capabilities. Enables a second, active site with duplicate, secure backups of critical configuration, policy, and key information—and secure recovery through Ingrian’s FIPS k-of-n smart card recovery mechanism.

About Ingrian’s CHOICE Architecture

This partnership with Ingrian and Princeton Payment Solutions is enabled through Ingrian’s CHOICE™ architecture, which represents the technology and core values that Ingrian offers to its customers. CHOICE is a flexible, integrated approach that allows customers to not only implement the solution they need today, but to leverage their investment to address future security and technological challenges—whether by adding new capabilities offered by Ingrian or its partners. The hallmark of CHOICE is the Ingrian KeySecure™ ISV Program, which outlines the framework for third-party product integration, providing developers with an open, extensible, and flexible environment for enhancing security and ease of use.

About Princeton Payment Solutions

Princeton Payment Solutions offers a range of products and services that enable organizations to improve the efficiency and security of payment processing in SAP R/3 environments, including enterprise resource planning (ERP) systems and retail automation applications. With their innovative suite of products, Princeton Payment enables organizations to automate credit card transactions, seamlessly integrate with the payment acceptance functionality in SAP, and to encrypt and secure the payment data in SAP. Ultimately, Princeton Payment improves the link between SAP-based businesses and their customers, making payment processing more efficient, more cost-effective, and more secure.

About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners, HighBAR Ventures, Menlo Ventures, Partech International, and Prism Venture Partners. For more information, visit www.ingrian.com.

© Copyright 2006 Ingrian Networks. The Ingrian Logo, Ingrian, and DataSecure are registered trademarks; and CHOICE and KeySecure are trademarks of Ingrian Networks. CardSecure is a registered trademark of Princeton Payment Solutions. All other brand names are trademarks of their respective holders.

ingrian-pps-sb-2006-09