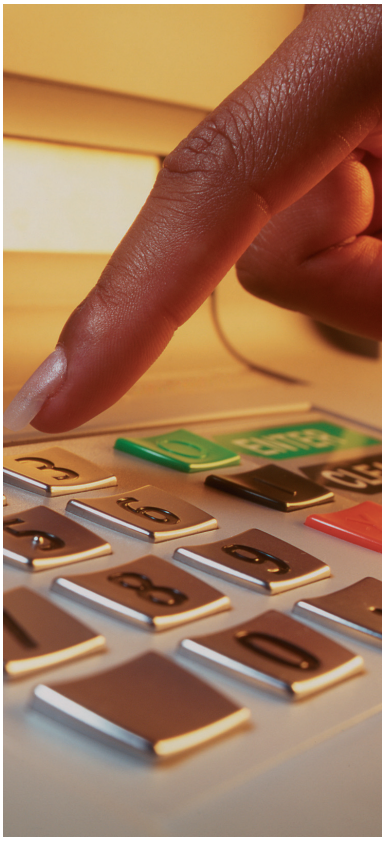
THALES

Maximize the use of your HSM 8000

Maximize the use of your HSM 8000

Table of Contents

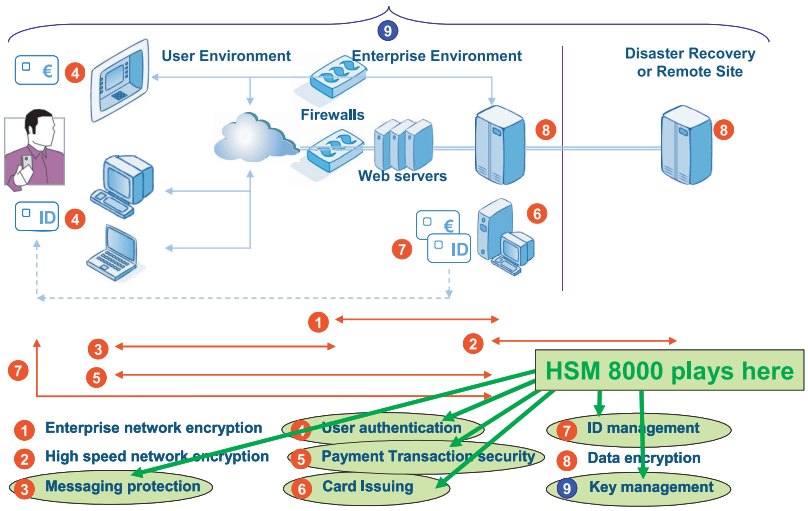


Executive Summary

Well designed and integrated security solutions are business enablers, not just IT infrastructure costs. Traditionally most banks and processors/switches use their payment hardware security modules (HSMs) almost exclusively for transaction processing. Increasingly Thales HSM 8000 customers are taking advantage of optional firmware features to maximize their investment. This delivers stronger security across a wide range of business needs, such as remote payment channels, data security, EMV card issuing and the emerging contactless card and mobile applications designed to replace low value cash payments. In today's competitive environment, banks that recognize how strong security can be a differentiator are gaining competitive advantage and ultimately market share.

This paper provides a high level overview of selected features available on the HSM 8000 platform. It explains how they can help in both reducing operating costs and enhancing existing or launching new authentication services to combat the growing threat of cardholder not present (CNP) fraud. Fully compatible with the flexible administration of the remote HSM management solution, Thales is enabling its customers to upgrade its installed base of HSM 8000 devices to support new industry initiatives that deliver consumer convenience while controlling risk and reducing fraud. Thales is the recognized global market leader in payment HSM security solutions and has embedded many features in its product today that will be mandatory components of security audits in the near future when the new Payment Card Industry (PCI) HSM standard is enforced.

Introduction



The diagram above indicates where the HSM 8000 can be utilized to deliver strong security throughout the enterprise.

New business applications

Most banks today have a strong desire to convert a large proportion of low value cash payments into electronic transactions. All of the leading card schemes, namely American Express, Discover, JCB, MasterCard and Visa, have launched their own variants of contactless credit/debit payment applications that can be used with smart cards and/or mobile phones. Market analysis of contactless technology, from organizations such as the Smart Card Alliance, shows a 'win' for all participants and the race is on by banks to secure pole position in the cardholder wallet.

The implementation of contactless issuing and transaction processing has been achieved largely without any major impact on existing payment infrastructures. The same applies to HSMs - a few additional cryptographic functions to support the specific processing requirements along the same networks used for magnetic stripe and EMV cards in the contact card world.

New applications or different uses for existing payment applications, most noticeably in transportation to replace proprietary fare collection systems, are expanding. Most banks need to run pilot projects to test customer acceptance before committing to a full scale rollout. The importance of early access to the latest security technology together with an optional customization service to create differentiation has never been more important.

Strengthening customer relationships

In the new world of increasing regulation, the contribution to the bottom line from credit card lending is likely to diminish in the short term. It is important to gain and maintain the trust of customers through a range of alternative payment offerings, which will deliver incremental revenue or reduce costs.

Despite the success of internet payment channels, widespread adoption is still being hindered by fears over online security. There are a number of different solutions available today, underpinned by the card schemes, which deliver additional levels of security, over and above the traditional username and password. Strong authentication solutions leveraging the EMV cards in circulation are increasing in popularity.

Today's consumer expects to be able to perform transactions securely using a wide variety of payment channels. It is the bank's challenge (and responsibility) to provide these options while safeguarding the customer data and identity. Banks who fail to meet this challenge, risk being left behind in the race for the new breed of consumer. Reducing time to market coupled with strong security is a pre-requisite for success.

Strong security

Strong security helps a financial institution build trust with its customers. It enables more services to be offered across lower cost payment channels.

The payment HSM is one of the most secure and trusted security devices in banking. It has been used for many years by the retail banking industry mainly during the transaction authorization phase. This is just a fraction of what the device can do - now is the time to leverage the HSM 8000 to deliver the new payment services that customers expect. There are a significant number of new features available, designed to simplify the management of a set of HSMs for multiple applications. This can be achieved across multiple sites if required and with the added advantage of strong adherence to existing and known future security audit requirements.

The remainder of this paper explains how the various features of the HSM 8000 can be used to deliver business benefits to the banking industry.

V

The Thales HSM 8000: More than just transaction processing

Targeting new customers

The HSM 8000 has proven it capability as a secure device for transaction switching and authorization. It has a multitude of additional cryptographic capabilities that can easily be deployed to assist with new applications and services that financial institutions want to offer their customers. This supports both the retention of existing customers and the capture of new customers.

The main areas where the HSM 8000 can play a major role in underpinning the security infrastructure and hence building customer trust are:

- Strong authentication for internet banking
- contactless card issuing and transaction processing to displace cash
- Strong data security to keep all keys and customer data secure - helping organizations to comply with the Payment Card Industry Data Security Standard (PCI DSS)

Leveraging the installed base of HSM 8000 devices reduces time to market and helps create competitive advantage.

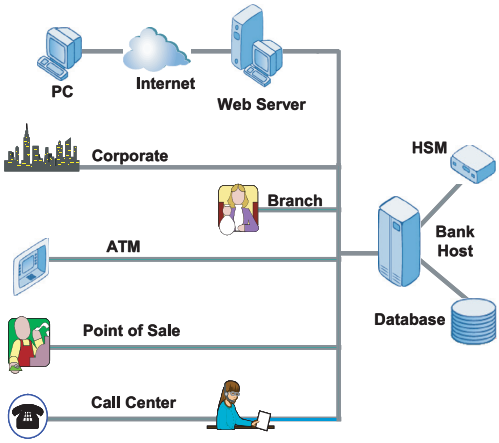
New features for new security needs

There are three main areas where improvements in security implementation are emerging. As part of its continuous evolution, the HSM 8000 has been enhanced in terms of features specifically to support:

- Control of critical cryptographic keys when outsourcing card production
- Elimination of key manipulation or substitution attacks
- Strong authentication to combat CNP fraud on Internet-based transactions

Before the introduction of EMV smart cards, many banks managed the complete card production process in-house. In the world of magnetic stripe cards this was feasible because the card configuration and cryptographic infrastructure for issuing was significantly less complex than that for EMV. In the drive to reduce costs, many banks chose to outsource the complete EMV card production to a third party bureau - they simply provided the traditional cardholder data (CHD) file and the bureau handled everything else. However, there is a better approach involving one simple additional step for the bank, which minimizes risk and provides greater business flexibility. Using the HSM 8000 for EMV data preparation is a cost effective solution.

Without adequate security procedures there are known weaknesses in some of the key management standards currently in use in the financial industry such as the American National Standards Institution (ANSI) X9.17 protocol. These relate mainly to the misuse of keys to encrypt/decrypt data and the substitution of one part of a key with another known key. Therefore, key storage and key exchange can be compromised even when strong algorithms, such as triple DES, are in use. Thales is an active contributor to the ANSI X9F working group and has updated the range of key management techniques in the HSM 8000 to reflect the latest ANSI publications which address the known weaknesses, namely X9.24 and TR-31.



The diagram above shows the various methods by which customers now expect to conduct payment transactions without fear of their card details or identity being compromised. The Branch, ATM and Point of Sale (POS) methods are well established and highly secure due to the physical presence of the cardholder together with a secure physical device (subject to formal audit approval) to accept the physical payment card. The other methods for payments are growing in popularity but they all share a common risk that the security infrastructure needs to mitigate - that is the fact that the cardholder is not present in front of a physical device that is trusted and controlled by the bank. Thales has various product options to offer to enhance the security of these payment methods, leveraging the existing cards and supplementing the infrastructure with additional low cost tokens or client software. It can be seen that whatever method of payment is used, the same HSM 8000 platform is used as the core security platform by the bank to authenticate the user.

Affordable flexibility

The range of functionality available on the HSM 8000 platform is segregated into separate modules under license control. This provides financial organizations with the flexibility to purchase just the modules they need to meet their exact business requirements. As an alternative to purchasing additional HSMs as the transaction volume increases, each HSM is capable of receiving a performance enhancement through a license update. Coupled with the fact that each HSM has the option of being managed from a remote location in addition to directly at the data centre, the security staff have considerable flexibility in providing on-demand management and diagnostics at reduced cost.

For processors and bureaus providing issuing and processing services on behalf of multiple banks, the ability to load multiple local master keys (LMKs) into a single HSM 8000 device delivers significant benefits in terms of key separation meeting the needs of both customers and auditors.

V

A license to win

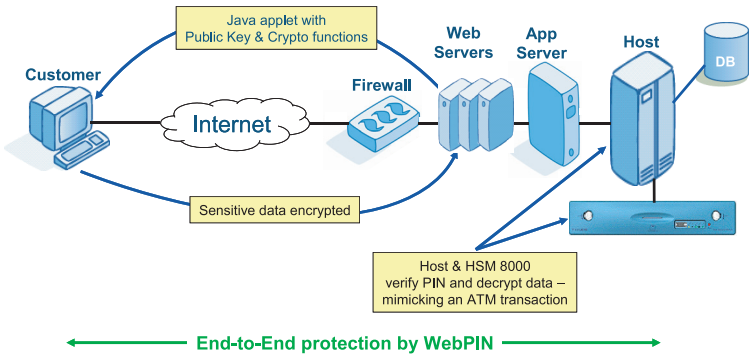
Authentication, authentication, authentication

Cardholder not present (CNP) fraud is increasing as other types such as counterfeit card fraud is decreasing due to the deployment of EMV cards. The HSM 8000 supports cryptographic functions to assist with the issuance of hardware/software tokens and the subsequent authentication of the user when using the appropriate payment channel.

The solutions are compatible with the industry offerings for EMV authentication (MasterCard Chip Authentication Program or CAP and Visa Dynamic Pass code Authentication or DPA) and 3D-Secure (Verified by Visa and MasterCard Secure Code). The **User Authentication** license provides all the cryptographic functions necessary to support both schemes.

CAP and DPA make use of a standalone handheld reader which has a smart card slot for the customer EMV card to be placed. Where available, this is being used by an increasing number of bank customers to provide high levels of security for applications such as phone banking, internet banking and on-line payments. For the early adopter banks, the incremental cost to upgrade the HSM installed base to support these features is minimal compared to the benefits to be gained in reduced operating costs, stronger security, brand image and customer retention.

Independent of the card schemes, Thales developed another innovative solution, specifically designed to leverage the existing bank investment in ATM PIN verification systems. **Web PIN** uses the HSM 8000 platform to provide high levels of security for on-line banking. The diagram below shows where Web PIN is deployed in the security infrastructure.



It provides an Internet end-to-end security envelope, employing banking industry standards combined with 'best of breed' internet security techniques - the key advantage is that no additional hardware is necessary at the client browser. By securing the important cardholder and PIN data right through to the HSM 8000, the traditional attacks on the web server are negated.

Web PIN supports three primary functions related to Internet banking for the following data sent to and/or received from the Web Server:

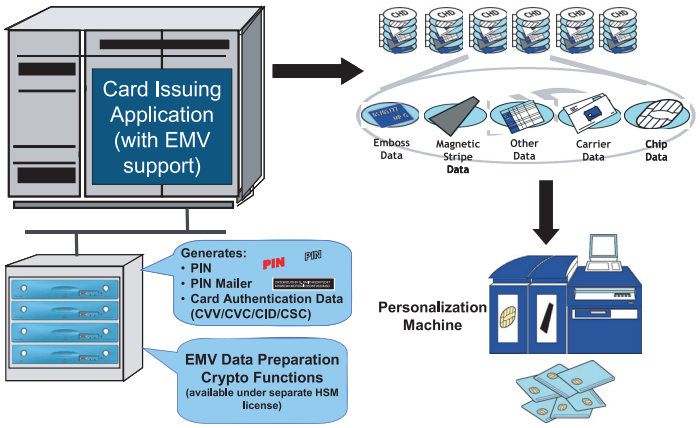
- PIN-based user authentication compliant with triple DES encrypted ANSI PIN blocks
- Message authentication using triple DES ANSI message authentication codes (MACs)
- Data privacy using triple DES encryption

For banks not wishing to issue hardware tokens to each of its customers, Web PIN provides a low cost but highly secure alternative making maximum usage of the existing HSM 8000 PIN verification infrastructure.

Take control of card issuing

To date, most implementations of EMV issuing systems have used an external data preparation solution which takes a legacy magnetic stripe data file and enriches it with EMV data prior to making it available to an in-house or external personalization facility. The market leading product in this category is the Thales Personalization Preparation Process or P3 for short. The key advantage of this approach is that there is no need to modify the legacy host application leading to reduced risk and fast time to market for banks just starting to introduce EMV compliant cards to their customers.

There is, however, increasing demand for an alternative approach to card issuing which involves the EMV data preparation process being tightly coupled to the host application. This makes use of the **EMV data preparation** license available on the HSM 8000 platform. The diagram below shows a typical deployment with a group of HSMs being used directly by a host application to create all the data necessary to produce all variants of EMV cards and applications.



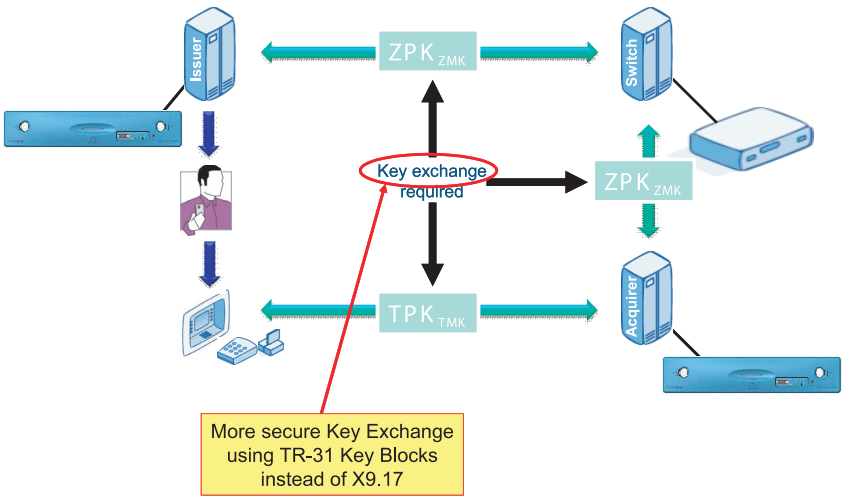
The functionality available in the HSM 8000 supports data preparation for all major card scheme applications on native (proprietary), Global Platform (sometimes referred to as Java card) and Multos smart cards. This enables the issuer to take complete control of all the important master keys and provides the flexibility to outsource card production to a third party bureau without the need to relinquish control of the top level keys. This means that there is limited risk of the issuer's reputation being damaged in the event of a security breach at the third party premises. It also provides the issuer with the capability to share the load of card production between multiple bureaus.

In addition to the standard data preparation license Thales offers a **Card Issuance Functionality** custom firmware which is used by system integrators to provide a complete in-house data preparation and issuing solution. Either solution provides issuers with complete control of the issuing process and enables future capabilities such as instant issuance or dynamic risk management to be realized. The Thales Professional Services team has valuable experience in working with individual banks on their EMV migration projects and are able to assist in developing additional firmware command to suit the particular host system in question.

No data loss here

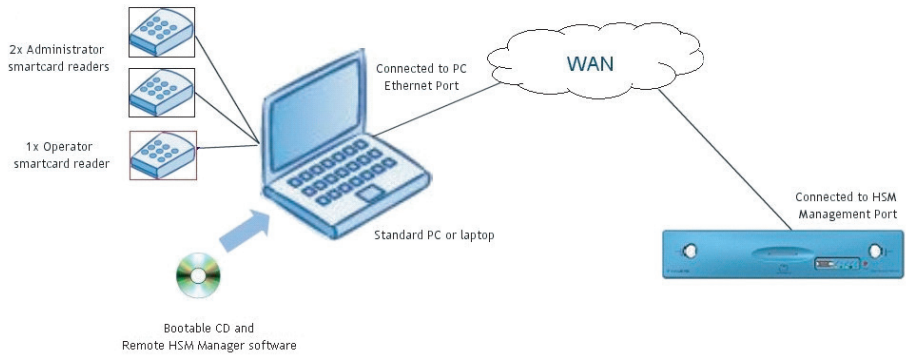
Using the **Message Encryption** license on the HSM 8000 provides a simple route to compliance for the Protect Cardholder Data section of the PCI DSS standard. This satisfies requirement 3 (protect stored cardholder data) and requirement 4 (encrypt transmission of cardholder data across open, public networks). Integration with the host application is very straightforward and the commands available enable easy interoperability with third party systems in terms of key exchange and method of encryption. Other complementary Thales solutions such as **CryptoStor** provide secure tape backup and retrieval mechanisms for critical data and can also assist with audit compliance.

The standard base software provides the capability to utilize ANSI X9.24 compliant key blocks as an alternative to the traditional variant LMK scheme employed in the HSM 8000 product line. Both key management schemes can be used in parallel. In addition the **TR-31** license provides a highly secure method of exchanging keys with third parties since it enforces proper key usage and eliminates key substitution attacks. Thales is an early adopter of this new technology and encourages banks to start migrating their key management to ANSI X9.24 and TR-31 as soon as possible. Various security audit requirements in the pipeline are likely to mandate stronger key management based on key blocks.



Simplify your security management

Standardizing on the HSM 8000 as the core security component in the organization helps to simplify the management task and is also highly likely to reduce operational costs. The recommended method to reduce costs is to enable the HSMs with the **Remote Management** capability. This provides highly scalable administration and eliminates most requirements to visit the data centre to perform HSM configuration or diagnostic tasks.



For third party processors and card bureau, the **Multiple LMK** license can significantly reduce the number of HSM groups required. Instead of just a single local master key (LMK) being available per HSM, up to 20 LMKs can be loaded per device. This opens up a wide range of permutations for handling different banks or groups of banks under separate LMKs. Without the multiple LMK capability this would have necessitated physically separate HSMs hence losing flexibility in terms of cost effective scalability as volume of transactions or cards increase. The solution is highly secure since each LMK has its own independent set of security/authorizing officers. Remote management is an ideal way to manage an HSM with this capability and offers the opportunity to implement a fast LMK rollover when necessary.

Conclusion

The table below summarizes the HSM 8000 licenses that apply to each of the business solutions mentioned in this paper.

	New payment applications	CNP payment channels	Securing data & messages	Card issuing
	Remote HSM Manager			
HSM 8000 Licenses	Included in base Licenses	User authentification Message encryption Multiple LMK Web PIN	Message encryption Multiple LMK TR-31	RSA contactless issuing EMV data preparation Multiple LMK TR-31
Complementary Thales applications	N/A	SafeSign family Web PIN client	CryptoStor	P3 PINMan

Remote HSM Manager adds flexibility and reduces cost in all cases. Transaction processing for all the latest credit and debit applications is traditionally included as part of the base license.

Maximizing the use of the Thales HSM 8000 provides:

- Significant operational cost savings
- Ability to launch new payment channels quickly underpinned by strong security
- Lower risk when outsourcing card production
- Reduced time to meet security audit requirements
- A range of new features through firmware upgrades - no need to replace the existing HSM 8000 installed base
- All features mentioned are available now - please contact the local Thales representative for more information

About Thales

Thales is a leading international electronics and systems group, addressing defence, aerospace and security markets worldwide.

Thales's leading-edge technology is supported by 22,000 R&D engineers who offer a capability unmatched in Europe to develop and deploy field-proven mission-critical information systems.

To this end, the group's civil and military businesses develop in parallel and share a common base of technologies to serve a single objective: the security of people, property and nations.

&partnerships with national customers and market players, while leveraging its global expertise to support local technology and industrial development.

Thales employs 68,000 people in 50 countries with 2007 revenues of €12.3 billion.

Thales
Security Solutions & Services
Information Systems Security

Europe, Middle East, Africa

Meadow View House
Long Crendon
Aylesbury
Buckinghamshire
HP18 9EQ. UK
Tel.: +44 (0)1844 201800
Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

Americas

2200 North Commerce Parkway
Suite 200
Weston, Florida
33326

Tel.: +1 888 744 4976 or +1 954 888 6200
Fax: +1 954 888 6211
E-mail: sales@thalesesec.com

Asia Pacific

Units 2205-06
22/F Vicwood Plaza
199 Des Voeux Road Central
Hong Kong, PRC
Tel.: +852 2815 8633
Fax: +852 2815 8141
E-mail: asia.sales@thales-esecurity.com

177A-062009A - Photos: iStockphoto, Thales

THALES