



Weston, 19th May 2008

Thales enhances HSM cryptographic security with Industry Standard Key Block Functionality

HSM 8000 version 3.0 provides users with greater security and flexibility, giving them better control over keys, and interoperability of key exchange using industry standards.

Thales, a leader in information systems security, today announced the launch of the latest version of its payment Hardware Security Module (HSM) software aimed at organizations within the global banking community. The new version offers enhanced security of key exchange between different parties in the payments network, as well as greater flexibility in how outsourced payment processors manage their payment HSMs and better security for local key management. Furthermore, version 3.0 is fully backward compatible, enabling existing customers to easily upgrade, minimizing disruptions to existing applications and systems.

Version 3.0 introduces support for the ANSI TR-31 interoperable key block format for key exchange. This brings compliance with ANSI X9.24, which replaces the older ANSI X9.17 standard. The TR-31 format also enhances security for key exchange between different parties in the payment network, including those using other vendors' HSMs that support TR-31. TR-31 is specified in the latest MasterCard and Visa backed PCI security requirements for exchanging keys with point of sales devices and ATMs.

The introduction of Thales key blocks for local storage under the Local Master Key (LMK) provides greater security through better control of the use of cryptographic keys. At the same time, the binding and integrity protection provided by key blocks make them resistant to a range of theoretical 'command manipulation' attacks. The combination of Thales and TR-31 key blocks creates a secure environment for local key storage and distribution.

The final enhancement addresses the increasing trend by banks to outsource their card acquiring and issuing activities. As payment processing outsourcers and bureaux serve many customers, they are under pressure to assure them that their keys are being kept secret and therefore separate from other customers' keys. The multiple LMK functionality within Thales HSM 8000 version 3.0 enables outsourcers, for the first time, to maintain cryptographic separation of all their clients' keys on the same HSM. Such functionality not only enhances security but also provides outsourcers with greater flexibility in terms of HSM



management as they can securely use a number of client keys on the same HSM and take on new clients without security concerns.

Paul Meadowcroft, Head of Transaction Security for the Information Systems Security activities at Thales, says: "As increasing computing power is available to enable criminals to attack systems, this latest functionality ensures payment HSM security stays two steps ahead of the fraudsters. We are making the upgrade process for existing customers as simple as possible by allowing a gradual migration to the new version. Once upgraded, customers will benefit from a state-of-the-art hardware security module which provides better key security and greater flexibility. As the market leader for payment HSMs and an active contributor to ANSI X9 and other standards bodies, we aim to lead industry requirements such as TR-31, to ensure our customers continue to receive the highest levels of protection."

With 70 percent of global transactions secured by Thales HSMs, the introduction of TR-31 and Thales key blocks, and support for multiple LMKs on a single payment HSM further enhances Thales's position as a leading provider of advanced security solutions.

ENDS

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. The group builds its growth on its unique multi-domestic strategy based on trusted 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 forecast 2007 revenues in excess of €12 billion.

Thales is a world leader in the provision of Information and Communication Systems Security solutions for all critical infrastructures including governments, the military, satellite networks, enterprises and the finance industry. Thales has 40 years of unrivalled track record in protecting information up to Top Secret and a comprehensive portfolio of products and services, which includes network and communications encryption, access control, remote user solutions, telephony as well as consulting, evaluation and accreditation. In the financial world, Thales secures value bearing transactions, data preparation for card and PIN issuing, and provides advanced user and message authentication solutions supported by secure identity management and token issuing. Over half of the world's banks, together with the majority of the busiest exchanges, currently use Thales technology and services. www.thalessec.com.

Press contacts

Chris Klein
Thales eSecurity
chris.klein@thalessec.com
+954-888-6200