

Thales Launches nShield Connect 6000 Hardware Security Module

Thales Extends Market-Leading Product Line to Set New Benchmarks for Performance, Scalability and Resilience in Delivering Critical Cryptographic Services

July 15, 2009 – Thales, leader in information systems and communications security, announces Thales nShield Connect 6000, the industry's fastest network-attached hardware security module (HSM) and the only one to offer dual, hot-swappable power supplies. nShield Connect 6000, part of the nCipher product line, meets business continuity and scalability requirements for mission-critical security systems that protect personal and other sensitive information – handling heavy workloads in even the most demanding always-on data centers.

HSMs are widely accepted as industry best practice for protecting cryptographic keys and for performing encryption and digital signing. HSMs provide a cost-effective way to increase the security of software-based systems, enforcing access control and key management policies within a tamper-resistant security environment. nShield Connect 6000 is a network-attached appliance that acts as a highly scalable, centralized resource for managing keys and protecting sensitive data for as many as 100 servers, virtual machines or other application instances – ensuring that policies are consistently applied and operational costs are significantly reduced. Like all Thales HSMs, nShield Connect 6000 is easily deployed to support a wide range of shared security infrastructure applications such as Microsoft Certificate Services (PKI), Entrust Authority Security Manager, RSA Certificate Manager, Oracle Database, and Microsoft SQL Server. nShield Connect 6000 is validated to FIPS 140-2 level 3, the most widely adopted security benchmark for cryptographic solutions in government and commercial enterprises.

nShield Connect 6000 is specifically designed with dual hot-swappable power supplies and field serviceable components to support the needs of high-capacity shared IT infrastructures within modern data centers, where resilience and ease of maintenance are a primary concern. Similarly, with the rapid adoption of encryption across the enterprise nShield Connect 6000 satisfies the ever increasing demand for performance by delivering the highest performance figures in the industry - processing up to 6,000 signing transactions per second¹ (TPS) with RSA 1,024-bit keys and even more importantly up to 3,000 TPS¹ when taking advantage of longer, more secure, 2,048-bit keys that are increasingly recommended by regulators and industry bodies.

“As fraud, data theft and other security breaches continue to make headlines, our customers consistently tell us that they have an ever increasing need for a high performance and resilient cryptographic infrastructure,” says Franck Greverie, Vice President, Managing Director for the information systems security activities of Thales. “nShield Connect 6000 complements the market leading nCipher product line and has been designed to meet the high availability and business continuity needs of our customers. I am delighted to demonstrate this commitment to the nCipher product line following Thales's successful acquisition of nCipher.”

nShield Connect 6000 provides a number of advanced benefits including:

- Unsurpassed business continuity and field serviceability – nShield Connect 6000 is the only hardware security module to offer dual power supply units (PSUs), helping customers to improve availability of their solutions by connecting the HSM to two independent power sources. One of the important benefits of the design is to enable servicing to be carried out in the field. The dual power supplies are hot-swappable, enabling customers to change one power supply at a time without having to interrupt services for maintenance tasks because the HSM doesn't have to be shut down or sent to a service center for repair. The unit also contains redundant, field-serviceable fans.
- Unique scalability – nShield Connect 6000 is the world's fastest network-attached HSM, processing up to 6,000 signing transactions per second (TPS) with RSA 1,024-bit keys. It has been optimized to deliver up to 3,000 TPS when taking advantage of longer, more secure, 2,048-bit keys that are increasingly recommended by regulators and industry bodies, such as the U. S. National Institute of Standards

Technology (NIST), the French Central Information Systems Security Division (DCSSI), and the German Federal office for information Security (BSI).

- **Reduced cost of ownership** – The inherent resiliency of nShield Connect 6000 and the ability to provide cryptographic services to as many as 100 application instances simultaneously (a five-fold increase over previous models) reduces the total cost of ownership. Customers are able to create a truly shared and robust infrastructure while purchasing fewer HSM devices, using less rack space and less power.
- **Powerful key management** – Acting as a centralized resource, nShield connect 6000 unifies key management policies and provides a single point from which to administer cryptographic keys, avoiding the need to visit remote servers. This addresses the costly and error-prone operational processes of key generation, rotation and recovery across distributed networks - costs that are further amplified when stringent supervision and audit rules are in force. nShield Connect 6000 fully supports the Thales Security World™ key management framework providing hardware-enforced dual controls and powerful separation of duties delivering enhanced governance and above all, confidence.
- **High security** – nShield Connect 6000 features a tamper-responsive chassis; its cryptographic components are validated to FIPS 140-2 level 3 and Common Criteria EAL 4+, positioning it for use in highly regulated environments.

nShield Connect 6000 is an extension to the nCipher product line and is fully compatible with existing Thales nShield and Thales netHSM products. Customers can mix and match these products under a common Thales Security World key management framework and utilize existing developer tool kits.

1 Performance may vary depending on operating system, application, network topology, and other factors.

About GEOBRIDGE

Since 1997, GEOBRIDGE has been providing information security solutions to global clients. Today our client list includes Fortune 500 companies, financial institutions, health care, government agencies and defense clients across North America and internationally. GEOBRIDGE helps clients mitigate risk and realize significant value from their IT investments while allowing clients to focus on the growth and profitability of their company. Our team provides solutions, integration services and consultancy in the areas of encryption, network security, identity management, transaction security, and compliance. Due to the increased needs for compliance with internal governance, and external legal and regulatory requirements, we have expanded our compliance and security best-practices offerings to address information assurance. GEOBRIDGE is a Qualified Security Assessor company (QSAC) certified by the Payment Card Industry (PCI) and a TG-3 Assessor recognized by the Electronic Funds Transfer (EFT) networks.