

nShield Edge Extends Enterprise-Grade Cryptographic Security

Fills gap in the marketplace between smart cards and traditional hardware security modules

April 27, 2010 - Thales, leader in information systems and communications security, announces nShield Edge, the world's first FIPS 140-2 Level 3 validated USB-attached hardware security module (HSM). nShield Edge combines the portability of smart cards with the high security and resilience of HSMs, enabling consistent key management outside the datacenter and across the enterprise.

nShield Edge, part of the nCipher product line, is one of the world's most compact HSMs, measuring only 120 x 118 x 27mm. It features an integrated card reader and requires only a standard USB connection to the host computer to operate. Designed for applications requiring portability combined with enterprise-grade security, nShield Edge fills a significant gap in the marketplace between portable smart cards and traditional datacenter HSMs.

Smart cards, commonly used for protecting personal credentials, are highly portable and provide physical protection for keys. However they typically lack the scalability, strong authorization controls, and key recovery capabilities required to support mission-critical enterprise applications. While HSMs offer these features, they are best suited to high performance datacenter deployments. nShield Edge offers a "best of both worlds" solution that is secure and portable to help organizations comply with best practices as they deploy dispersed encryption and digital signature-based applications.

"As cryptography becomes more widespread to secure data and ensure consumer privacy, enterprises demand new form factors to employ key management best practices across the extended enterprise." says Franck Greverie, vice president for the information technology security activities of Thales. "nShield Edge enables enterprises to conveniently and cost effectively extend the same level of security found inside the datacenter to applications like offline certification authorities, registration authorities, code signing, remote HSM operations, and development environments."

nShield Edge offers organizations a number of distinct advantages. Due to its small size, nShield Edge has the optimal form factor for use on the road, in temporary deployments, in remote offices or placed in vaults for high assurance applications that require strong physical security while they are off-line. Because it connects via a USB port and does not require an additional power supply, nShield Edge is well suited for use with laptops. In addition, HSM protected keys and cryptographic operations within nShield Edge can be accessed by virtual machines since many hypervisors can pass the USB connection through to the guest operating system.

Common Applications

Financial services, high technology, government, retail and healthcare sectors are expected to use nShield Edge in the following ways:

- **Remote office deployments** – nShield Edge hardware is easy to install or retrofit to existing servers, making it a good choice for distributed data protection. The Thales Security World key management framework enables remote and automated provisioning of keys to remote locations without the need for security personnel to travel to the site.
- **Offline Certification Authorities** – nShield Edge is the ideal form factor for offline Certification Authorities (CAs), which are underpinned by some of the most valuable key material in an enterprise's infrastructure. With nShield Edge it is possible to protect the root keys in an HSM that is small enough to be stored safely in a physical vault when not in use.
- **Code Signing and other high assurance digital signatures** – nShield Edge supports the typical laptop or workstation environment and is the perfect source of trusted signatures, even if quorum

based user signing is required. Effective key backup and recovery features ensure long-term code signing keys cannot be lost.

- **Remote authorization for HSMs** – nShield Edge is the ideal form factor to allow remotely located security personnel to authenticate and authorize administrative activities to other remotely located nShield HSMs. This task would typically be performed from a workstation or laptop environment and requires an HSM to be attached to the remote user's workstation.
- **HSM application development** – The size, form factor and compatibility of nShield Edge makes it ideal for application developers wishing to validate their application with Thales HSMs, especially if the developer is using a laptop – making it the ideal personal HSM for developers at their desks.

The introduction of nShield Edge extends Thales's nShield product portfolio and complements existing embedded (nShield Solo) and network connected (nShield Connect) HSM solutions. All are fully compatible with each other and support comprehensive disaster recovery, key sharing between HSMs and the use of strong authentication for administrators, dual controls and clear separation of duties. Keys and meta information can be automatically backed up without requiring additional hardware or on-site presence, reducing the total cost of operations.

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.