



## Hardware Security Solutions for Microsoft SQL Server 2008

### SOLUTION BRIEF

#### Solution Benefits

- Increased security through separation of cryptographic keys from encrypted data
- Data can be encrypted by using keys that only the database user has access to on the external EKM/HSM
- Simple Windows-based installation of SafeNet Extensible Key Management feature
- Cost-effective extensibility of Microsoft platform
- Designed for HSM Best Practices
- Code Module Signing
- Transparent Data Encryption (TDE) support
- FIPS 140-2 Level 3 validated
- Enables users to meet PCI DSS standards
- PKI root key protection

SafeNet Hardware Security Modules are the first to integrate with Microsoft SQL Server 2008 for robust key management and encryption, delivering unprecedented levels of data security, performance and compliance.

#### First HSM to work with Microsoft SQL Server 2008

SafeNet is the first HSM vendor to work with Microsoft SQL Server 2008, a relational database management system that provides organizations with a highly secure data platform for storing and managing sensitive data. Unlike its predecessor releases, Microsoft SQL Server 2008 enables the use of third-party HSM devices for storage of keys and cryptographic operations, such as key creation, deletion, encryption, and decryption for complying with security best practices and PCI DSS mandates.

Integration of SafeNet's Luna SA with Microsoft SQL Server 2008 allows storage of the server's master cryptographic keys—the foundation of any robust security solution—within the hardware and not the software, and provides greater application security and performance by offloading select key management functionality. The high-assurance Luna SA provides a verifiable audit trail as evidence that your keys have been properly secured throughout their entire life cycle.

In addition to the Luna SA, the SafeNet Luna PCI, a high-security cryptographic PCI accelerator card, can also be integrated with Microsoft SQL Server 2008. When embedded directly into the database server, the Luna PCI provides added security, as well as accelerated cryptographic performance and CPU offload.

#### How it Works

SQL Server 2008 introduced Extensible Key Management (EKM) for managing keys outside of SQL Server. Traditionally, all symmetric and asymmetric Keys used by SQL Server reside in the database itself, however EKM allows key creation, storage, encryption and decryption to be done outside the database using an HSM. To use this feature SafeNet (the EKM provider) wrote a module which implements certain interfaces that SQL Server uses for key management and cryptographic operations. Key creation and management DDL supports key creation using EKM providers.

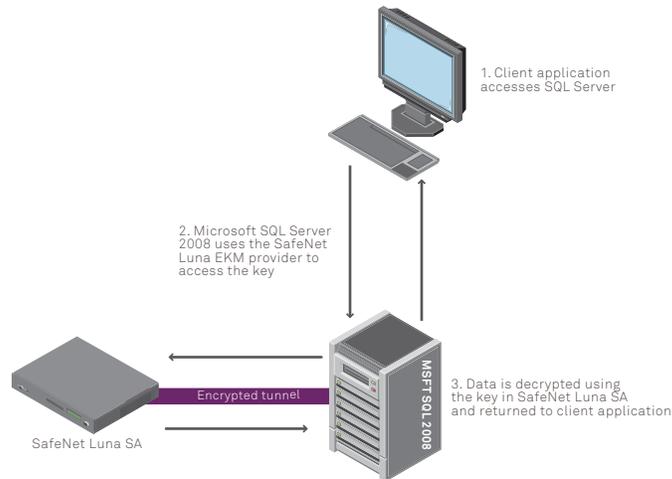
#### Ease of Integration

The SafeNet Luna SA and Luna PCI offer users of Microsoft SQL Server 2008 two flexible encryption options for their deployment scenarios. The Luna SA is a network-attached HSM that connects to the server through TCP/IP. It can be leveraged by many servers, offering the ability to securely partition and share the HSM resource, and is a cost-effective way of extending the data platform. The Luna PCI is a PCI-card form factor HSM that connects to the server in the PCI bus and provides seamless deployment to a wide range of security applications. Its full cryptographic application program interface support makes integration quick and easy.

“SafeNet’s Luna SA provides organizations using SQL Server 2008 additional security features to help meet today’s ever-evolving data threats and compliance mandates. Organizations can add a layer of security technology that protects keys to be separate from the data it protects while accelerating complex features such as key rotation.”

~ Mark Jewett  
 Director of SQL Server Marketing,  
 Microsoft

Integration with Microsoft applications is facilitated via the SafeNet Luna EKM, which is used to set up Extensible Key Management (EKM) for Microsoft SQL Server 2008. Initializing the SafeNet Luna EKM ensures all keys that are generated via SQL Server 2008 or transparent data encryption (TDE) will be stored on the SafeNet HSM. The Luna EKM Configuration Utility allows the flexibility to set parameters required by the EKM module, and thus specify a particular HSM and slot number. Data can be encrypted by using encryption keys that only the database user has access to on the external Luna EKM module.



### Enterprise Data Protection

SafeNet HSMs are a key component of SafeNet’s comprehensive Enterprise Data Protection (EDP) solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet EDP is the only solution that secures data across the connected enterprise, from core to edge, providing protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited “islands” of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit [www.safenet-inc.com/EDP](http://www.safenet-inc.com/EDP).

### Related Documents

Product Brief: SafeNet Luna SA

Product Brief: SafeNet Luna PCI

Press Release: SafeNet Offers First Hardware Security Module to Work with Microsoft SQL Server 2008

Solution Brief: SafeNet HSMs for Microsoft Certificate Services



**Microsoft** Partner

Gold Independent Software Vendor (ISV)  
 Silver OEM Hardware

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [www.safenet-inc.com/connected](http://www.safenet-inc.com/connected)

©2011 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. SB (EN)-03.21.11