SafeNet Securing Microsoft Solutions
SafeNet and Microsoft work closely to enhance the security of Microsoft solutions.
Active Directory Certificate Services

The Microsoft Active Directory Certificate Services on Windows provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure.

Organizations use certificates to enhance security by binding the identity of a person, device, or service to a corresponding private key. However, in order to realize the enhanced security made possible by certificates, organizations need a cost effective, efficient, secure way to manage the distribution and use of certificates.

With Microsoft CA organizations have a fully integrated Public Key Infrastructure (PKI) service, secure Intranet, Extranet, Virtual Private Network (VPN) eMail and network logon. Microsoft CA solutions can enable a number of security services needing strong authentication and non-repudiation of transactions.

**Microsoft and SafeNet Security Solution Benefits:**

- Securely generate, store, and protect sensitive encryption keys
- Accelerate cryptographic operations
- High-level security for users private credentials & digital certificates. Users can authenticate, encrypt, sign and decrypt electronic transactions with full confidence.
- Two-factor authentication is enabled for a variety of network security applications, ensuring a high level of security through reliance on a hardware based USB device.
- Private keys and certificates, stored on the eToken, operate transparently with any standard browser and any Microsoft CAPI supported application such as eMail applications, VPN clients or network logon clients.
- Provide Audit trail for critical material
- Centralize key management and lifecycle
- Best practice for Risk Mitigation
- Non-repudiation of systems and transactions
- Limitation of access to sensitive data

Designed to meet the performance and assurance needs of the most demanding applications, SafeNet offers a full spectrum of encryption technologies for Microsoft applications to secure digital identities, data, communications, and transactions.
SQL Server 2008 R2 delivers several breakthrough capabilities that will enable your organization to scale database operations with confidence, improve IT and developer efficiency, and enable highly scalable and well managed Business Intelligence on a self-service basis for your users. Download the SQL Server 2008 R2 November CTP, as well as Microsoft’s complete Business Intelligence platform, including the new PowerPivot for Excel 2010.

**SafeNet Data Protection Products for Microsoft:**

**HSM**

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 previous 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 R2 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 R2. When embedded directly into the database server, the Luna PCI provides added security, as well as accelerated cryptographic performance and CPU offload.

**DataSecure**

SafeNet DataSecure appliances are the heart of all SafeNet data encryption and control solutions. Using hardware-based encryption, DataSecure appliances cover the broadest variety of data types. They provide a unified platform with data encryption and granular access control capabilities that can be applied to databases, applications, mainframe environments, and individual files. By providing centralized management of keys, policies, and essential functions, DataSecure simplifies administration, helps ensure compliance, and maximizes security.

**Microsoft and SafeNet Security Solution Benefits:**

- Process large volumes of events across multiple data streams in less than a second
- Better manage your business through historical data mining and continuous insights
- Provides built-in support for different types of event handling and rich query semantics
- Reduce development cost by utilizing existing skill sets and investments in Microsoft development platform
- Tailor to needs of the business with flexible deployment options
- Reduce cost and complexity of management with a platform that is easy to manage and support
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
Forefront Identity Manager

Microsoft® Forefront Identity Manager 2010 Certificate Management (FIM CM) is Microsoft's registration authority and certificate management system. The previous version of FIM 2010 was known as Identity Lifecycle Manager 2007. It blended Microsoft Identity Integration Server (MIIS) 2003 with Certificate Lifecycle Manager (CLM). FIM 2010 natively supports Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 certification authorities (CAs) for the issuance of the certificates. FIM 2010 can programatically support third-party CAs as well, if your organization has not deployed Microsoft CAs.

SafeNet Data Protection Products for Microsoft:

HSM

To achieve the appropriate level of trust, enterprises using Microsoft Forefront Identity Manager 2010 Certificate Management (FIM CM) implement a CA hierarchy and take advantage of specialized hardware in the form of hardware security modules (HSMs) to protect the private key material of the issuing CA. SafeNet Luna SA HSM can be easily integrated with Microsoft FIM 2010 to enhance the overall security of the solution by:

- Securely storing the master admin key within the secured HSM enclosure thereby protecting the agent private keys that are used by FIM CM
- Storing the global platform master keys for applet management operations
- Diversifying the master admin key and creating a different admin key for each smart card in the organization
- Securely authenticating to the smart card with its admin key to perform management operations
- Random Number Generator for server key generation

Microsoft and SafeNet Security Solution Benefits:

- Process large volumes of events across multiple data streams in less than a second
- Better manage your business through historical data mining and continuous insights
- Provides built-in support for different types of event handling and rich query semantics
- Reduce development cost by utilizing existing skill sets and investments in Microsoft development platform
- Tailor to needs of the business with flexible deployment options
- Reduce cost and complexity of management with a platform that is easy to manage and support
SharePoint

SharePoint 2010 is the business collaboration platform that enables you to connect and empower people through formal and informal business communities, within the enterprise and beyond, and to manage content throughout the information lifecycle. Whether deployed on-premises or as hosted services, SharePoint's integrated capabilities are enhanced by search technologies and enable you to rapidly respond to changing business needs by making data-driven decisions and by deploying customized solutions quickly and securely. The consolidation of collaboration solutions onto SharePoint 2010 makes it possible to cut costs by lowering training and maintenance expenses and increasing IT productivity, all within a governable and compliant platform.

SafeNet Data Protection Products for Microsoft:

HSM

The SharePoint Security solution will be a combination of Active Directory Rights Management Services, SQL Server 2008 Transparent Database Encryption and SSL using Internet Information Services (IIS) 7.0. A single HSM (Luna SA) will be deployed to provide a security framework to the data in use, data at rest and the data in transit.

Microsoft Office SharePoint Server 2007 will use Microsoft Active Directory Rights Management Services to implement document security utilizing Luna Cryptographic Service Provider (CSP) to store the AD RMS cluster keys on Luna SA and Microsoft SQL Server 2008 for Transparent Database Encryption utilizing Luna Extensible Key Management (EKM) to encrypt the Office SharePoint Server 2007 database(s) with the asymmetric key on Luna SA. Moreover, the AD RMS cluster web site and SharePoint web sites are hosted on Microsoft IIS 7.0, therefore Luna Key Storage Provider (KSP) can be utilized to store the SSL keys and certificates on Luna SA.

SafeWord 2008

SafeWord 2008 two-factor authentication protects your most important assets and applications. SafeWord’s easy-to-use tokens and seamless integration with your existing Microsoft infrastructure make it simple to deploy two-factor authentication for VPNs, Citrix applications, Web applications, Webmail, and Outlook Web Access.

eToken

SafeNet’s range of certificate –based (PKI) USB authenticators provides a broad and versatile offering for organizations, allowing them to architect for choice by selecting and centrally managing a range of different authentication solutions for diverse groups of users, depending on their usability needs and risk levels. SafeNet’s USB certificate-based authenticators can be used on any computer with a USB port and require no reader. They meet the highest security standards including FIPS 140-2 and Common Criteria, and enable compliance with security regulations including HIPAA, HSPD-12, SOX, GLBA, FFIEC, Basel II, PCI and HITECH. SafeNet’s certificate-based USB authenticators enable remote access, network access as well as other advanced applications including digital signing, password management, network logon and proximity.

Microsoft and SafeNet Security Solution Benefits:

- Protecting Data at Rest
- Protecting Data in Transit
- Securing web services
- Audit and compliance
- SSL Key Storage for IIS Server and acceleration
- Transparent Database Encryption for SharePoint Server Databases
- Secure cryptographic Key Management
Protection you need.
Quality you Deserve.
Rights Management Services

Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use.

SafeNet Data Protection Products for Microsoft:

HSM

Enhance Microsoft security solutions with SafeNet hardware security modules (HSMs). Designed to meet the performance and assurance needs of the most demanding applications, SafeNet HSMs add dedicated cryptographic acceleration and hardware key management to Microsoft applications that secure digital identities, data, communications, and transactions.

Microsoft and SafeNet Security Solution Benefits:

- Limiting access to sensitive data
- Strong security
- Non repudiation of systems or transactions
- Centralised key management and key life cycle
- Paper to digital processing archiving
Unified Access Gateway

Forefront Unified Access Gateway 2010 (UAG) delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors on both managed and unmanaged PCs and mobile devices. Utilizing a combination of connectivity options, ranging from SSL VPN to DirectAccess, as well as built in configurations and policies, UAG provides centralized and easy management of an organization's complete anywhere access offering.

SafeNet Data Protection Products for Microsoft:

**eToken**

SafeNet's range of certificate-based (PKI) USB authenticators provides a broad and versatile offering for organizations, allowing them to select and centrally manage a range of different authentication solutions for diverse groups of users, depending on their usability needs and risk levels. SafeNet's USB certificate-based authenticators can be used on any computer with a USB port and require no reader. They meet the highest security standards including FIPS 140-2 and Common Criteria, and enable compliance with security regulations including HIPAA, HSPD-12, SOX, GLBA, FFIEC, Basel II, PCI and HITECH. SafeNet's certificate-based USB authenticators enable remote access, network access as well as other advanced applications including digital signing, password management, network logon and proximity.

<table>
<thead>
<tr>
<th>Microsoft and SafeNet Security Solution Benefits:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Strengthen VPN security for remote access</td>
</tr>
<tr>
<td>• Protect data on laptops and PCs</td>
</tr>
<tr>
<td>• Enhance network access security</td>
</tr>
<tr>
<td>• Simplify password management and protection</td>
</tr>
</tbody>
</table>
**Acceleration Server**

Microsoft Internet Security and Acceleration (ISA) Server 2006 is an integrated network edge security gateway that helps protect IT environments from Internet-based threats, while providing users fast and secure remote access to applications and data. Microsoft Forefront Threat Management Gateway (TMG) is a comprehensive Secure Web Gateway solution that helps protect employees from Web-based threats. It also delivers simple, unified perimeter security with integrated firewall, VPN, intrusion prevention, malware inspection and URL filtering.

**SafeNet Data Protection Products for Microsoft:**

**HSM**

Enhance Microsoft security solutions with SafeNet hardware security modules (HSMs). Designed to meet the performance and assurance needs of the most demanding applications, SafeNet HSMs add dedicated cryptographic acceleration and hardware key management to Microsoft applications that secure digital identities, data, communications, and transactions.

**Microsoft and SafeNet Security Solution Benefits:**

**Luna SA for SSL enhances ISA Server SSL sessions with:**

- Reduced bottlenecks at the webserver to increase traffic volumes
- Reduced web page loading times
- Capacity to set up over 1200 new SSL connections per second per module
- Shared SSL acceleration between multiple IIS servers
- SSL Hardware Key Management
- Luna SA for SSL manages multiple SSL private keys within secure hardware
- Secure SSL private keys in hardware that meets the widely recognized FIPS 140 security benchmark for cryptographic hardware
- Advanced protection for cryptographic keys critical to maintaining the confidentiality of each SSL session and the integrity of the web site's identity
- Luna SA for SSL rates high on both the performance and security axes to guarantee that SSL sessions are responsive and immune to hacking and fraud
- Physical and logical isolation of key materials from the TMG server prevents the extraction of key materials
**Authenticode**

Enhance Microsoft security solutions with SafeNet hardware security modules (HSMs). Designed to meet the performance and assurance needs of the most demanding applications, SafeNet HSMs add dedicated cryptographic acceleration and hardware key management to Microsoft applications that secure digital identities, data, communications, and transactions.

Microsoft™ Authenticode™ permits end users to identify who published a software component and verify that no one tampered with it before downloading it from the Internet. Authenticode assures end users of the identity of the software publisher and that the code has not been altered after the signature was applied, before they download signed code from the Internet.

Authenticode relies on proven cryptographic techniques and the use of one or more private keys to sign and time-stamp the published software. It is important to maintain the confidentiality of these keys.

**SafeNet Data Protection Products for Microsoft:**

**HSM**

The SafeNet Luna Hardware Security Module (HSM) integrates with Microsoft Authenticode to provide a trusted system for protecting the organizational credentials of the software publisher. The SafeNet Luna HSMs secures the code-signing key within an industry standard FIPS 140-2 level 3 validated HSM.

**SafeWord 2008**

SafeWord 2008 two-factor authentication protects your most important assets and applications. SafeWord's easy-to-use tokens and seamless integration with your existing Microsoft infrastructure make it simple to deploy two-factor authentication for VPNs, Citrix applications, Web applications, Webmail, and Outlook Web Access.

**Microsoft and SafeNet Security Solution Benefits:**

- Non repudiation of systems or transactions
- Best Practises and risk mitigation
- Audit and compliance
- Protection of IP
- Protection of brand
Online Certificate Status Protocol (OCSP)

OCSP is a protocol, which is used to provide real-time validation of a certificate’s status. An OCSP responder is used to respond to certificate status requests and can issue one of the three responses:

- Valid
- Invalid
- Unknown

The online responder service implements the Online Certificate Status Protocol (OCSP) by decoding revocation status requests for specific certificates. The service evaluates the status requests for these certificates and sends back a signed response containing the requested certificate status information.

SafeNet Data Protection Products for Microsoft:

HSM

Enhance Microsoft security solutions with SafeNet hardware security modules (HSMs). Designed to meet the performance and assurance needs of the most demanding applications, SafeNet HSMs add dedicated cryptographic acceleration and hardware key management to Microsoft applications that secure digital identities, data, communications, and transactions.

Microsoft and SafeNet Security Solution Benefits:

The Luna SA can be used for a number of Microsoft applications spreading cost across the infrastructure without compromising security

- Increased performance for OCSP
- Increased security for certificates
- Assured integrity and non repudiation
Active Directory

Active Directory provides the means to manage the identities and relationships that make up your organization's network. Integrated with Windows Server 2008 R2, Active Directory gives you out-of-the-box functionality needed to centrally configure and administer system, user, and application settings.

SafeNet Data Protection Products for Microsoft:

SafeNet ProtectDrive

SafeNet ProtectDrive is the most cost-effective and easy to manage disk and server encryption solution. ProtectDrive delivers the ultimate protection for sensitive data on laptops, workstations, and servers through robust data encryption. ProtectDrive is the most Microsoft-centric disk encryption product available. Not only does ProtectDrive tie into Microsoft Active Directory, it leverages Active Directory directly as its administration platform, reducing deployment and management time, as well as direct costs.

eToken

TMS has an open, standards-based architecture, based on configurable connectors for integrating with a wide variety of security applications. Recognizing the inherent complexity and the needs facing network and IT managers charged with managing user and security services, TMS was developed based on the proven Microsoft Active Directory framework. Although based on Active Directory, TMS can also be operated in a stand-alone mode, allowing the organization to use any standard user management system.

SafeWord 2008

SafeWord 2008 is designed for the Windows 2008 Server environment. SafeWord enables you to leverage both 32-bit and 64-bit Windows operating systems, including Vista, Windows 2008 Server, as well as Windows 2003 and XP. As you upgrade your Microsoft Windows infrastructure, SafeWord two-factor authentication will be there, fully integrated and ready to help you drive productivity and security. SafeWord 2008 server runs on 32 and 64 bit versions of Windows 2003 and Windows 2008 Seamless Active Directory Integration. - SafeWord installs in minutes and offers seamless integration with Microsoft Active Directory, making the administration of authentication activities easy and predictable. Token registration, user accounts and enrolment, and administrative activities are managed right in the Microsoft Management Console, using your existing Active Directory accounts. Once your users have been properly authenticated with their SafeWord token, you can rely on the same Active Directory listings that you use every day to determine what applications, data, and network resources each user can access.

Microsoft and SafeNet Security Solution Benefits:

- Utilisation of Active Directory infrastructure
- Utilisation of Active Directory Security Policies and Procedures
- Time and Cost Reduction
- Equipment Cost Reduction
- Ability to use in-house knowledge base for managing 3rd party products
- Ease of use and familiarity
- Security and Authentication products run on already integrated system
SafeNet is a global leader in information security, founded more than 25 years ago. The Company protects identities, transactions, communications, data and software licensing through a full spectrum of encryption technologies, including hardware, software, and chips. More than 25,000 corporate and government customers in 100 countries including UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service, trust their security needs to SafeNet. In 2007, SafeNet was acquired by Vector Capital, a $2 billion private equity firm specializing in the technology sector.

SafeNet Data Protection Solutions for Total Information Lifecycle Protection

SafeNet solutions deliver persistent protection of information at critical points in its lifecycle, wherever and however that information gets used. SafeNet solutions equip customers with the agility they need to adapt to change and act on opportunity. SafeNet delivers these comprehensive capabilities:

- Strong authentication and identity management solutions that protect identities for users and servers
- Industry-validated, hardware-based encryption platforms that protect transactions, ensure data integrity, and maintain an audit trail
- Data encryption and control solutions that protect and maintain ownership of data throughout its lifecycle—from the data center to the endpoint and into the cloud
- High-performance communications encryption solutions that persistently protect information, ensure control beyond location or boundary, streamline operations, and reduce compliance costs
SafeNet, a Microsoft Gold Partner

SafeNet is proud to announce that we have renewed our Microsoft Gold Partnership for 2010 Gold Certified Partners represent the highest level of competence and expertise with Microsoft technologies and have the closest working relationship with Microsoft.

Contact Us

Corporate Headquarters:
4690 Millennium Drive
Belcamp, Maryland 21017 USA
Tel: +1 410 931 7500 or 800 533 3958
Email: info@safenet-inc.com

EMEA Headquarters:
Tel: +44 (0) 1276 608 000
Email: info.emea@safenet-inc.com

APAC Headquarters:
Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com

Follow Us:
www.safenet-inc.com/connected

©2010 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.