# Table of Contents

**Introduction** ..............................................................................................3

**The Role of Security in Modern Business** ................................................4

  - Microsoft’s best practices for trustworthy computing ........................................ 4
  - Gemalto offers data-centric security ................................................................. 5
  - Gemalto’s basic encryption and key management principles .............................. 5

**The Gemalto Portfolio of SafeNet Encryption and Key Management Products** .............................................................................................................. 6

  - SafeNet KeySecure ............................................................................................. 6
  - SafeNet ProtectV ................................................................................................. 6
  - SafeNet High Speed Encryptors ......................................................................... 6

**Establishing Roots of Trust** ......................................................................7

  - Gemalto root of trust products: security in hardware ......................................... 7

**The Challenge: Remaining Agile While Mitigating Risk—on the Premises and in the Cloud** ............................................................................................................. 8

  - Securing identities with authentication ............................................................ 8

**Working Together: Microsoft Products and SafeNet Solutions** ..............10

  - Microsoft Active Directory products and SafeNet solutions ........................... 11
  - Microsoft Forefront Protection Suite and SafeNet solutions ........................... 12
  - Microsoft Forefront Threat Management Gateway and SafeNet solutions .... 14
  - Microsoft SharePoint and SafeNet solutions .................................................... 14
  - Microsoft Authenticode and SafeNet solutions ................................................ 15
  - Microsoft Online Certificate Status Protocol (OCSP) and SafeNet solutions .... 15
  - Microsoft Office 365 and SafeNet authentication solutions ................................ 16
  - Microsoft Office 365 and SafeNet High Speed Encryptors ............................... 16
  - Microsoft Azure and SafeNet ProtectV ............................................................ 17
  - Microsoft SQL Server 2012/2014 and SafeNet HSMs ........................................ 17
  - Microsoft Products and SafeNet authentication solutions .................................. 18
  - Microsoft Solutions and SafeNet HSMs .......................................................... 18

**For More Information** .............................................................................19
Introduction

Since the modern era of computing, Microsoft Corporation has been a foundational provider of software applications that organizations have relied on heavily to conduct all aspects of their businesses. Programs such as Microsoft Word, Excel, PowerPoint, Outlook, Publisher, Office 365, and more have been a part of virtually every business for as long as people could place their hands on a keyboard. So foundational are these programs that it’s safe to say they are part of the backbone of modern enterprise IT, and, as such, serve as a core element of an enterprise’s functional identity. By providing a basis for company content and information to be developed, shared, and used to grow and expand business, Microsoft’s software applications play an important role in driving corporate efficiencies and allowing enterprises to allocate and optimize resources across market segments.

An untold quantity of confidential information and records are stored within these programs such as data accumulated over decades and increasing exponentially every moment around the globe. As such, the vast amount of data stored within these applications, individually and collectively, is part of the core of an organization’s storage infrastructure.

Microsoft takes their role in business life seriously. Knowing the risks of cloud-enabled environments, Microsoft has made security a critical part of their development efforts by including and improving security measures over the years.

Gemalto supports Microsoft’s efforts by lending its expertise in data encryption, enterprise key management, and authentication. When Microsoft’s products are deployed using Gemalto’s complementary security solutions, enterprises benefit from additional safeguards to their sensitive data at rest and in motion, improved security around enterprise applications, and a robust security posture that makes demonstrating regulatory compliance easy. Through its products, Gemalto enhances the security measures of Microsoft storage environments for the purpose of protecting organizations and their data, which is the very lifeblood of their business.
The Role of Security in Modern Business

Whether you collect competitive information, customer personally identifiable information, client email addresses, payment details, research, or intellectual property, properly securing your data is essential. Businesses that do not completely and comprehensively secure their data will incur significant costs when their data is lost or stolen. Due to the increase and the level of sophistication of attacks, a breach in data security is not a question of if but when. And, when that breach occurs, the consequences can severely damage the reputation and performance of even the strongest organizations.

Microsoft’s best practices for trustworthy computing

Microsoft’s trustworthy computing initiative strives to make a safer, more trusted cloud environment. To that end, Microsoft has articulated three elements that guide their efforts:

Fundamentals

Even before a product is ever conceived, Microsoft trains its developers, testers, and program managers to use the Trustworthy Computing Security Development Lifecycle (SDL) approach to building software code in order to make online activities, software, and services safer. Once deployed, Microsoft follows through on its commitment to security by continually enhancing the processes and tools used for updating and improving customer software.

Threat and Vulnerability Mitigation

Microsoft reduces an enterprise’s attack exposure through in-depth comprehensive approaches to defense that use best-in-class threat protection, detection, and removal products. Their software and technology portfolio addresses enterprise security needs through central visibility and control of risk, and seamless integration with a wide range of IT systems.

Identity and Access Control

Ensuring that users represent themselves appropriately is an essential part of Microsoft’s innovation and integration strategies. Their solutions ensure that users accessing enterprise resources are trustworthy. Additionally, they aim to give administrators the tools they need to manage policies that dictate which resources each user can access in order to protect information permanently, wherever it is stored.

Gemalto supports Microsoft’s efforts by lending its expertise in data encryption, enterprise key management, and authentication. When Microsoft’s products are deployed using Gemalto’s complementary security solutions, enterprises benefit from additional safeguards to their sensitive data at rest, improved security around enterprise applications, and a robust security posture that makes demonstrating regulatory compliance easy.
Gemalto offers data-centric security

Gemalto takes a data-centric approach when enhancing Microsoft’s efforts at trustworthy computing. Authentication and key management directly address identity and access management risks, while encryption technologies eliminate the risks to sensitive data regardless of where it resides. These technologies and approaches secure critical points in business operations so that organizations remain protected, compliant, and in control of their resources.

This eBook highlights solutions that enable security teams to centrally employ defense-in-depth strategies. Inadequate access controls can compromise the value of encryption deployments. Easily forged identities open network resources to theft or sabotage. And, vulnerable cryptographic keys make for vulnerable data—even if it is encrypted.

Gemalto’s robust access controls, strong identity management, and comprehensive encryption management are practical, cost-effective, and comprehensive tools that enhance the security in Microsoft’s product portfolio. Encryption of data, while it is at rest or in motion, is an effective means of securing data. Experts recommend using encryption and enterprise key management1 to:

> isolate regulated and sensitive information
> separate encryption control from data center management

Separating encryption and enterprise key management duties from the administrative responsibilities of managing the storage infrastructure ensures that no internal user will have universal, unfettered access to secured data. Additionally, implementing encryption and key management according to best practices centralizes the monitoring of the security deployment and makes audit reporting easier for the enterprise. Not only does this approach secure sensitive data, it has the added benefit of streamlining administrative and regulatory processes.

Why are encryption and key management recommended so highly? One reason is that they render secured data useless to attackers—unlike other security measures that leave sensitive data in cleartext. Gemalto’s data-centric approach means that wherever the data resides, it is protected against unauthorized use. Strong perimeters and robust authentication deployments are important components of any security strategy; encryption protects resources in the event that any other component of the security strategy is breached. Associated key management adds an additional layer of granularity that allows organizations to divide data access according to such factors as business policy, job responsibilities, or location. Whether threats originate internally or externally, encryption and key management offer robust security and nuanced, yet clear, control of sensitive data.

Gemalto’s basic encryption and key management principles

By putting sensitive data into encrypted cipher text, organizations assume a greater level of control over their data by controlling the ability to unscramble it. If unauthorized users get access to the secured data, it will remain useless without the appropriate decryption key. Additionally, separating encryption management responsibilities from the general maintenance of the data center adds an extra layer of data security that addresses the risk posed by insiders. By enforcing the separation of duties that compliance mandates require, encryption becomes a multi-pronged security tool that secures data and mitigates threats from external and internal threats.

In addition to securing data at rest and in motion, encryption can be used to granularly apply security policies to specific subsets of data in databases and applications. Encryption secures data as it progresses through workflows, and safeguards it when it is manipulated by processes running within a virtual machine instance; for example, fields containing sensitive data in a web application.

Encryption key management at the enterprise level can present significant challenges—particularly if there are multiple, disparate encryption and key management deployments and no formal key management policies in place. Key storage, rotation, and deletion requirements add costs and administrative overhead. Administrators, amid the complexity of their deployments, have been known to store and manage keys insecurely; for example, it has been reported that some have stored their keys in spreadsheets on USB drives. On the other hand, many administrators are dealing with multiple legacy or inherited key management systems. Regardless, without a dedicated key management system, it has been difficult for administrators to consistently adhere to the enterprise key management best practices.

1 Recommending organizations include the National Institute of Standards and Technology (Source: NIST, Guide to Storage Encryption Technologies for End User Devices, http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf) and Gartner (Source: Gartner, Simplify Operations and Compliance in the Cloud by Encrypting Sensitive Data, August 15, 2013, retrieved from http://www.gartner.com/document/2576198. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.)
The Gemalto Portfolio of SafeNet Encryption and Key Management Products

**SafeNet KeySecure**

SafeNet KeySecure is a key management platform that centralizes the control of an organization’s disparate encryption solutions. Streamline security administration by consolidating policy and key management of application servers, databases, storage, file servers and virtual. SafeNet KeySecure’s centralized key management improves security by making key surveillance, rotation and deletion easier, while also separating duties so that no single administrator is responsible for the entire environment. SafeNet KeySecure also is integral to the connectors. Only Gemalto delivers key management FIPS 140-2 Level 3 or 1 validated hardware, or a virtual appliance with a hardware root of trust using SafeNet Hardware Security Modules, across traditional and virtualized data centers, and public cloud environments.

SafeNet KeySecure provides you with complete control of your encryption keys, and ultimately your data, ensuring that no one else can access your data without your knowledge or permission.

**SafeNet ProtectV**

SafeNet ProtectV provides full disk encryption of virtual machine instances so you can securely run even your most sensitive workloads or any highly regulated data in the cloud. Ensuring cloud-enabled security, SafeNet ProtectV is the industry’s first comprehensive high-availability solution for protecting data across virtual and cloud infrastructures. SafeNet ProtectV encrypts entire virtual machine instances and attached storage volumes, keeping your data safe from unauthorized access. In addition, no virtual machine instance can be launched without proper authorization from SafeNet ProtectV StartGuard™ pre-boot authentication. With SafeNet ProtectV’s unified encryption and access control, your organization can be safe knowing that you retain access to and control of your encrypted data and keys at all times.

You can enhance your business agility and take advantage of the lower costs inherent in virtual environments. Together with SafeNet KeySecure, SafeNet ProtectV provides a highly available encryption solution to address numerous industry security standards and government regulations such as PCI DSS and HIPAA HITECH. Regardless of where your workload resides, you can separate security administration duties, enforce granular controls and establish clear accountability with audit trails and detailed compliance reporting.

**SafeNet High Speed Encryptors**

As more sensitive assets traverse networks from site to site and across data centers, on-premises, and in private and public clouds, organizations need to know that their data in motion is secure, especially in multitenant, geographically distributed environments. The SafeNet family of high speed encryption (HSE) products comprises tamper-proof hardware appliances with internal key vaults designed to provide confidentiality for information transmitted over Ethernet networks.

Field proven, the SafeNet HSE high-assurance encryptors provide the assurance of FIPS, Common Criteria and CAPS (UK) certified security for specific models. In addition, the solutions have been vetted by such organizations as the Defense Information Systems Agency (DISA UC APL) and NATO. Designed to support the growing need to encrypt data in motion, SafeNet High Speed Encryptors secure sensitive data more efficiently than higher layer protocols, thereby lowering the cost of network security and compliance. Suited to the most demanding environments, SafeNet High Speed Encryptors ensure the lowest overheads on resources, enabling scalable, cost- effective secure network connectivity that grows as bandwidth requirements increase.
Establishing Roots of Trust

Roots of trust, as defined by the Cryptographic Technology Group at the US National Institute of Standards and Technology (NIST), are components that are inherently trusted to perform one or more security-critical functions. Protecting cryptographic keys, performing device authentication, or verifying software are just three examples. These components must be secure by design and, according to NIST, ideally implemented in or protected by tamper-resistant hardware.

Gemalto root of trust products: security in hardware

When encryption keys are stored in hardware security modules, they are protected from the reach of unauthorized users. Whereas software-stored encryption keys can be more easily copied, stolen or deleted, hardware-stored keys can be tightly controlled, protected from compromise, and easily audited. Encryption materials stored in tamper-proof hardware appliances can be trusted to serve as a secure root of trust for all of an infrastructure’s cryptographic operations.

Root of Trust: SafeNet HSMs

SafeNet HSMs are robust, high-availability, high-performance appliances that ensure the integrity of cryptographic operations by issuing, validating, and storing encryption keys and certificates in a protected environment. Its FIPS 140-2 Level 3 tamper-resistant design ensures that stored materials cannot be compromised; and since encryption keys never leave the appliance, organizations can rest assured that only authorized users have access to the cryptographic material securing their resources. Additionally, SafeNet HSMs are capable of performing thousands of cryptographic transactions per second, offering the throughput and responsiveness to support the most demanding SSL applications.

Managing Roots of Trust: SafeNet Crypto Command Center

Securely and easily manage SafeNet HSMs and cryptographic resources from one central location, regardless of the use case, with SafeNet Crypto Command Center. Cost-efficiently manage crypto services, and expand IT infrastructure in physical, cloud, hybrid cloud, and virtual environments. As the market’s first true crypto hypervisor, encryption services are delivered in minutes versus days, while you maintain full control of encryption services and data. Additional benefits include: better High Availability (HA) management, improved client visibility, and enhanced resource management through crypto resource reporting, as well as secure multi-tenant even in public cloud environments.

Encryption materials stored in tamper-resistant hardware appliances can be trusted to serve as a secure root of trust for all of an infrastructure’s cryptographic operations.

Securing identities with authentication

Organizations can now increase productivity and reduce costs by allowing decentralized user access to enterprise resources from numerous endpoints. But, how do organizations know that users are who they claim to be? Lost or stolen credentials can pose significant security risks as resources move beyond the traditional data center.

Remotely delivering applications or storing data have made conducting business easier than ever. Yet, an additional password becomes required each time a resource moves beyond the data center’s perimeter. Each new password represents a target for thieves and a weak link in the security chain. As workforce mobility trends increase, organizations will need to examine how they secure their applications and information.

Organizations ensure that users are correctly identified by deploying multi-factor authentication. Multi-factor authentication solutions add an extra layer of identity verification—an exchange of material or information that only the appropriate user knows. Assigned security certificates, biometric information, or cryptographically generated one-time passwords valid for a single use can be used in varying forms to assure a user’s identity with a high degree of confidence. With multi-factor authentication, lost or stolen passwords or tokens are useless without the additional piece of information that serves as the second factor of identity verification.

Multi-factor authentication offers flexible deployment options that can suit any organization’s needs. Cloud-based authentication-as-a-service models are economical alternatives adapted to trends in user mobility. It’s important to choose a platform that can improve the way that administrators deploy and manage their authentication infrastructure. Policy-based controls, automation, and integration with existing identity management systems (such as Active Directory) are features that administrators can use to reduce risks while preserving a positive user experience. For end users, mobile tokens, hardware tokens, smart cards, mobile PKI Bluetooth readers, and other authentication methods can be the right mix of ease, convenience, and security.
SafeNet authentication solutions

Gemalto’s suite of SafeNet authentication solutions integrate with a wide range of Microsoft products to ensure that only authorized users gain access to their enterprise’s valuable resources.

SafeNet Authentication Service
The SafeNet Authentication Service delivers fully-automated, highly secure, cloud-based authentication-as-a-service for enterprises and service providers. With support for a wide breadth of authentication methods, SafeNet Authentication Service protects a broad IT eco-system, including SaaS applications, VDI, VPNs, web portals and local networks. SafeNet Authentication Service offers streamlined management and shared services with its multi-tier multi-tenant environment and automated workflows, making secure access in cloud and mobile environment easy and painless.

SafeNet Authentication Manager
SafeNet Authentication Manager is a versatile authentication server that manages all of an organization’s PKI certificate, lifecycle, and authentication needs from a single back-end platform. SafeNet Authentication Manager supports a broad range of authentication methods and form factors, including context-based authentication with step-up capabilities to OTP, OOB, PKI, X.509 certificate-based tokens and software tokens, so organizations can meet different assurance levels and address numerous use cases.

SafeNet MobilePKI
SafeNet MobilePKI Office uses Bluetooth Smart technology to enable connectivity for roaming users, integrating with desktop and mobile devices for anytime, anywhere PKI security on PCs, tablets and smartphones. SafeNet MobilePKI Office enables secure mobility by integrating seamlessly with existing ecosystems and extending typical PKI-based corporate badge solutions and PKI security to mobile devices. For enterprises that have already deployed PKI, the same credentials can be used to validate the identity of users on all Windows enabled desktops and mobile devices. This allows enterprise users to log onto corporate resources, and sign documents or email on their mobile devices and PCs using a token or badge that communicates via Bluetooth with all PKI applications.

SafeNet Authentication Service and SafeNet Authentication Manager both support a wide portfolio of authentication methods [e.g. out-of-band (OOB), hardware- and software-based one-time password (OTP) form factors] so organizations can choose the type of authentication that best meets their needs. In addition, their support of third-party authenticators means that enterprises can update their authentication systems without sacrificing their existing investments. By combining SafeNet Authentication and AD FS, lost or stolen passwords are rendered insufficient for accessing an enterprise’s sensitive information.
### Working Together: Microsoft Products and SafeNet Solutions

<table>
<thead>
<tr>
<th>Microsoft Solutions</th>
<th>SafeNet Solutions</th>
<th>Encryption and Key Management</th>
<th>Roots of Trust (HSM)</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Certificate Services</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Rights Management Services</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Active Directory Federated Services</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>Forefront Identity Manager</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>Forefront Threat Management Gateway</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Forefront Unified Access Gateway</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>SharePoint</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>Authenticode</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Online Certificate Status Protocol (OCSP)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Office 365</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>SQL Server</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
</tr>
<tr>
<td>Azure</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Microsoft Active Directory products

Microsoft Active Directory Certificate Services

Microsoft Active Directory Certificate Services (AD CS) is a management tool for the administration of cryptographic materials used in public key infrastructures (PKI). More specifically, AD CS is the service that provides the core functionality for Windows Server's certification authority (CA). Certificates enhance security by assigning the identity of a person, device, or service to a specific private key to ensure proper identity verification during sensitive cryptographic transactions. For organizations that rely on PKI, AD CS offers a cost-effective, efficient, secure way to manage the distribution and use of these certificates.

Fundamental to the integrity of this infrastructure is the CA's root cryptographic signing key, which is used to sign the public keys of certificate holders and its own public key. The compromise of a CA's root key either by malicious intent or by accident can have catastrophic consequences. Best practice dictates that this root-signing key be diligently stored in a tamper-resistant hardware security module (HSM).

Organizations that use AD CS in their infrastructure can store their encryption keys and certificates in SafeNet hardware security modules. In addition, certificates issued by AD CS can also be provisioned to SafeNet smart card authentication tokens for certificate-based authentication, and managed in SafeNet Authentication Manager.

Microsoft Active Directory Rights Management Services

Microsoft Active Directory Rights Management Services (AD RMS) is an information protection server that safeguards digital information from unauthorized use. Through the use of encryption, content owners using AD RMS can define which users have access to and can take actions on their content (for example Word documents, email, web pages, etc.). Its close integration with Active Directory identity management tools make it easy to assign access privileges to users in an organization. Additionally, usage policies travel with the files so access controls remain in place regardless of the file's location.

AD RMS secures files from a wide range of products including Microsoft Office, SharePoint, Exchange Server, Internet Explorer and Internet Information Services (IIS).

AD RMS users can deploy SafeNet HSMs to securely store the encryption keys used in protecting digital content. Keeping RMS encryption keys in the HSM's tamper-resistant appliance means that only authorized users will ever have access to the keys necessary for accessing secured digital content. Since master encryption keys never leave the appliance, only authorized users can get the keys they need to decrypt RMS protected files. SafeNet preserve the security of secured files by keeping the keys necessary for properly accessing data out of harm's way.

Microsoft Active Directory Federation Services

Microsoft Active Directory Federation Services (AD FS) is a tool installed on Windows servers that provides users throughout an enterprise with single sign-on (SSO) access to network and cloud-based resources. AD FS verifies user identities based on an exchange of private and secure information generated from a variety of authentication technologies—including PKI certificate-based authentication, OTP, OOB, and pattern-based authentication—generated from a wide variety of form factors, such as hardware, software, or mobile tokens, as well as Bluetooth Smart-based solutions. When users authenticate to AD FS, they need only sign in once to receive access to multiple web applications over the life of a single online session.

SafeNet security for Microsoft Active Directory products

SafeNet Hardware Security Modules

SafeNet HSMs integrate with AD FS to secure the token signing and certificate private keys. Preserving the token signing and certificate keys in a SafeNet HSM, organizations preserve the integrity of the authentication transaction. Since these materials never leave the hardware appliance, unauthorized users never have access to the materials they would need to steal to impersonate an authorized user. When a SafeNet HSM serves as the secure root to the SSO infrastructure, organizations can rest assured that identity verification transactions will be uncompromised.

SafeNet Authentication

SafeNet authentication solutions by Gemalto integrate with AD FS, enabling organizations to implement strong authentication for AD FS supported clients and web-based applications, such as Office 365. Acting as the trusted identity provider, SafeNet authentication solutions extend Active Directory identities to AD FS-supported environments.

SafeNet authentication solutions integrate with the Gemalto AD FS agent to provide the authentication mechanism for its SSO features. Through Gemalto’s AD FS agent, organizations can implement strong authentication policies for AD FS-supported clients and web-based applications.
Microsoft Forefront Protection Suite
Microsoft Forefront Unified Access Gateway

Microsoft Forefront Unified Access Gateway (UAG) provides secure remote access to corporate networks for employees, partners, and customers. UAG uses Secure Socket Layer (SSL), Virtual Private Network (VPN), Web application firewalls, and secure endpoint management to securely deliver web-based enterprise applications. Using UAG, enterprise applications are securely available to authorized users from anywhere.

SafeNet security for Microsoft Forefront United Access Gateway

SafeNet Hardware Security Modules

SafeNet hardware Security Modules integrate to store the certificates and encryption keys at the heart of UAG’s SSL transactions. With SafeNet HSM as the root of trust, organizations can securely send data and deliver applications through protected SSL tunnels. Data is encrypted before it travels and the keys necessary to decrypt it never leave the hardware appliance.

SafeNet Authentication

SafeNet Authentication solutions integrate to verify user identities as they log on to enterprise networks via UAG. By adding multi-factor authentication from Gemalto, enterprises strengthen VPN security which ensures that only authorized users gain access to private networks. Additionally, SafeNet Authentication Service and SafeNet Authentication Manager’s back-end management tools simplify ongoing administration of the authentication infrastructure for improved efficiency.
Microsoft Forefront Identity Manager

Microsoft® Forefront Identity Manager (FIM) is an identity management system that allows administrators to centrally manage identities and credentials across an enterprise in order to streamline administration and facilitate the enforcement of corporate policies. Close integration with Microsoft Active Directory and Exchange Server means administrators can effectively manage credentials from a central point so that it is easier to ensure that only appropriate users have access to sensitive materials. Additionally, detailed auditing capabilities, automated full lifecycle identity administration and self-service features combine to reduce the amount of time spent on help desk calls and audit reporting.

SafeNet security for Microsoft Forefront Identity Manager

SafeNet Hardware Security Modules

SafeNet Hardware Security modules (HSMs) integrate to protect the private keys and certificates that are assigned to users to verify their identities. When administrators store these materials in a SafeNet HSM, they ensure that the materials are never exposed outside of the HSM and are always protected from unauthorized users. By building the FIM certificate management infrastructure with the SafeNet HSM as the secured root, administrators ensure the integrity of all of their identity verification transactions.

SafeNet Authentication

SafeNet authenticators by Gemalto enable FIM users to store or create private digital credentials inside a number of form factors ranging from tokens to smartcards for easy, secure and portable authentication. From the central FIM console, administrators can provision, update and de-provision the authenticators used in their enterprise. Gemalto’s broad range of form factor support (including authenticators from third parties), coupled with FIM’s centralized identity management tools significantly reduces the complexity and expense of implementing and managing multi-factor authentication. An integration with SafeNet Authenticators strengthens an enterprise’s identity verification processes to ensure that only authorized users have access to sensitive enterprise materials.
Microsoft Forefront Threat Management Gateway

Microsoft Forefront Threat Management Gateway (TMG) is a secure web gateway that unifies multiple layers of security into an easy-to-use solution that protects against advanced web-based threats. Forefront TMG inspects web traffic at the network, application, and content layers so users can safely and productively use network resources without worrying about persistent threats. Beyond its ability to monitor web traffic for viruses and malware, it can serve as a firewall and VPN to secure access to internal resources. An SSL feature set secures internal communications through encryption so sensitive enterprise resources remain visible only to authorized users. TMG can be deployed either as a stand-alone server to deliver maximum performance, or as a virtualized machine combined with other applications to reduce capital investments.

SafeNet HSMs integrate with Forefront TMG to secure SSL transactions by storing master SSL private key in a FIPS 140-2 Level 3 tamper-resistant hardware appliance.

Microsoft SharePoint and SafeNet solutions

Microsoft SharePoint is a collaboration and file sharing platform that facilitates content management and communication throughout an enterprise. Available as an on-premises deployment or as a hosted service, SharePoint offers flexible deployments to match the needs of small and large scale enterprises alike. The ability to consolidate resources from disparate collaboration solutions onto SharePoint makes it possible for administrators to reduce training and maintenance expenses while also increasing IT productivity.

For organizations needing to secure SharePoint deployments, SafeNet HSMs serve as the trusted root for the encryption features offered by Microsoft Active Directory Rights Management Services (AD RMS), Microsoft SQL Server, and Microsoft Internet Information Services (IIS). Despite the use of multiple Microsoft encryption solutions, a single SafeNet HSM can store keys from the disparate deployments to provide a security foundation to data in use, at rest, and in motion.

While encryption secures data as it resides in SharePoint, organizations need to take steps to ensure that only authorized users have access to the data on the platform. SafeNet authentication solutions integrate with SharePoint to secure front-end access via strong authentication. By adding an extra layer of identity verification, organizations reduce risks posed by lost or stolen passwords and prevent unauthorized users from accessing important materials. Available in a cloud-based or on-premises deployment, SafeNet authentication is flexible enough to meet any of an organization’s needs.
Microsoft Authenticode and SafeNet solutions

Microsoft Authenticode permits end users to verify the authenticity of software code before downloading it from the Internet. Authenticode relies on the use of private keys to sign and time-stamp software during publication.

SafeNet HSMs integrate with Microsoft Authenticode to secure the cryptographic materials that sign code and prove authenticity of authorship. SafeNet HSMs are FIPS 140-2 Level 3 validated, tamper-resistant devices that preserve the integrity of code-signing operations by ensuring that the cryptographic materials used in the signing process remain secure.

Microsoft Online Certificate Status Protocol (OCSP) and SafeNet solutions

Microsoft Online Certificate Status Protocol (OCSP) is used to validate a certificate’s status in real-time. Using OCSP, administrators manage and distribute revocation status information on certificates in PKI environments.

OCSP integrates with SafeNet HSMs to verify, and revoke if necessary, certificates residing in the hardware security module.
Microsoft Office 365 and SafeNet Authentication Services

Microsoft Office 365 delivers standard Office applications and files directly from the cloud for flexible yet reliable access to the applications that enterprises depend on. With Office 365, user applications and files are consistently available whether the user is offline at their desk, online, or on a mobile device. Office 365 supports both Windows and Mac operating systems.

SafeNet authentication solutions seamlessly integrate so organizations can leverage Office 365’s flexibility while significantly reducing the risk of unauthorized access to corporate resources stored or run in the cloud. Using the Microsoft Active Directory Federation Services (AD FS), SafeNet authentication hardens access to Office 365 by adding a second layer of identity verification to ensure that only authorized users gain entry to protected applications. If AD FS is used for multiple cloud applications, SafeNet authentication solutions can unify authentication policies for the entire IT environment making identity verification easy across the entire enterprise.

Regardless of the endpoint being used to access documents, applications, or intellectual property residing in Office 365, with SafeNet authentication, only authorized users will be able to gain access. Now organizations can enjoy the benefits of delivering their Office applications from the cloud without having to worry about the identity of the users accessing them.

Microsoft Office 365 and SafeNet High Speed Encryptors

SafeNet High Speed Encryptors ensure secure communications to and from Microsoft Cloud for the utilization of Microsoft Office 365 and other applications. Enabling secure cloud connectivity, SafeNet High Speed Encryptors provide proven high-assurance Layer 2 network security for sensitive data, real-time video and voice, as it moves across virtual and physical networks, between data centers, to the last mile, and up to the cloud and back again. Securing data in motion across Layer 2 Ethernet connections, the solution is ideal for customers that require their Microsoft hosted services traffic to be encrypted as it moves between data centers. This capability ensures the data in motion is secure regardless of whether the information is flowing from the private to the public network or from the public to the private network, and that the security policy remains consistent.

Gemalto delivers world-leading certified high speed network encryptors for speeds up to 10 Gbps. Gemalto ensures best-in-class data-in-motion protection, maximum performance, near-zero overhead with “set and forget” management, and low total cost of ownership. SafeNet high speed encryption solutions protect data in motion, including real time voice and video streams, as well as metadata for enterprise and government organizations.
Microsoft Azure and SafeNet ProtectV

Businesses are increasingly turning to elastic cloud services like Microsoft Azure to run business-critical applications, but security and compliance remain top concerns. SafeNet ProtectV for Microsoft Azure solves this challenge by delivering a simple and easy way to protect even the most sensitive and highly regulated data on Microsoft Azure. Available on the Microsoft Azure Marketplace, SafeNet ProtectV secures sensitive and highly regulated data by encrypting entire virtual machine instances and attached storage volumes so data is safeguarded and completely isolated from Microsoft Azure, other tenants, and any other unauthorized parties. SafeNet ProtectV also ensures that no virtual machine instance can be launched without proper authentication from SafeNet ProtectV StartGuard pre-boot authentication. In addition, all of the data in archives is encrypted, including snapshots or virtual machine instances are tracked and are impossible to instantiate without authorized access.

With SafeNet ProtectV, enterprises across many verticals, including major financial institutions and governments, can securely run their workloads in the cloud while maintaining compliance requirements and achieving high levels of data protection.

Try SafeNet ProtectV on the Microsoft Azure Marketplace FREE for 30 days.

- 100 Nodes http://bit.ly/2cVpskZ
- 200 Nodes http://bit.ly/2cR0mHw

Microsoft SQL Server 2012/2014 and SafeNet HSMs

Microsoft SQL Server is a powerful relational database that enables organizations to scale operations with confidence, improve IT and developer efficiency, and effectively manage business intelligence on a self-service basis. With SQL Server, enterprises can process large volumes of data in fractions of a second making data mining and near instant insights easy.

SafeNet HSMs integrate with Microsoft SQL Servers to securely store encryption keys and manage such cryptographic operations as key creation, deletion, SQL encryption, and SQL decryption. Adding a SafeNet HSM allows administrators to store SQL server’s master cryptographic keys within a protected hardware appliance and not on the same software platform where encrypted data is stored. Verifiable audit trails act as a deterrent and serve as evidence that keys are properly managed and secured throughout their entire lifecycle to make demonstrating compliance easier.

Verifiable audit trails act as a deterrent and serve as evidence that keys are properly managed and secured throughout their entire lifecycle to make demonstrating compliance easier.
Microsoft Products and SafeNet Authentication Solutions

SafeNet authentication solutions provide front-end identity verification for a number of Microsoft products.

Organizations have a wide variety of authentication options that address the challenges posed by workforce mobility and password proliferation. SafeNet authentication solutions offer flexible service delivery that simplifies implementation and management. Automated processes significantly reduce the time and cost of provisioning, administering, and managing users and tokens compared to traditional authentication models.

SafeNet authentication solutions secure access to the following Microsoft products:

- Active Directory Federated Services
- Azure virtual desktops
- Azure Access Control Service
- BitLocker
- Direct Access
- Forefront Identity Manager
- Forefront Threat Management Gateway
- Forefront Unified Access Gateway
- HCK
- Internet Authentication Service (IAS)/Network Policy Server (NPS)
- Internet Information Services (IIS)
- Internet Security and Acceleration (ISA) Server
- Office 365/Office 365 Pro Plus
- Outlook Web Access
- Outlook Web App
- PuTTY
- Remote Web Workplace
- RD Web Access (RDWeb, formerly TSWeb)
- SharePoint
- Strong Name Tool
- Web Application Proxy
- Windows Logon
- Windows 2008R2 SSTP (Secure Socket Tunneling Protocol)

Microsoft Solutions and SafeNet HSMs

Designed to meet the performance and assurance needs of the most demanding applications, Gemalto offers a full spectrum of encryption and PKI technologies for Microsoft applications to secure digital identities, data, communications, and transactions.

- Active Directory
- Authenticode
- Microsoft Identity LifeCycle Manager
- Microsoft Certificate Enrollment
- SQL Server
- SharePoint
- Windows Rights Management System
- Microsoft Threat Management Gateway
- Microsoft Azure
- Online Certificate Status Protocol
For More Information

Microsoft’s commitment to Trustworthy Computing is unquestionable. Their focus on security fundamentals, threat mitigation, and identity controls preserve the integrity of their customers’ systems and data and make cloud operations internet safer for enterprises.

Gemalto, a global leader in data security and a Gold Certified Microsoft Partner, has many solutions that enhance security in Microsoft offerings. For over 30 years, Gemalto has been securing and protecting the valuable data assets and intellectual property of Fortune 500 global corporations, government agencies, and other organizations.

Gemalto’s data-centric approach for sensitive information focuses on the protection of high-value information throughout its lifecycle. Thousands of customers trust Gemalto to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

For more information regarding Microsoft and SafeNet identity and protection solutions by Gemalto visit: https://safenet.gemalto.com/partners/microsoft/
ABOUT GEMALTO ENTERPRISE SECURITY

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.