SafeNet security enhancements for **IBM solutions**

SafeNet

THE DATA PROTECTION COMPANY

Contents

The Role of Security in Modern Business

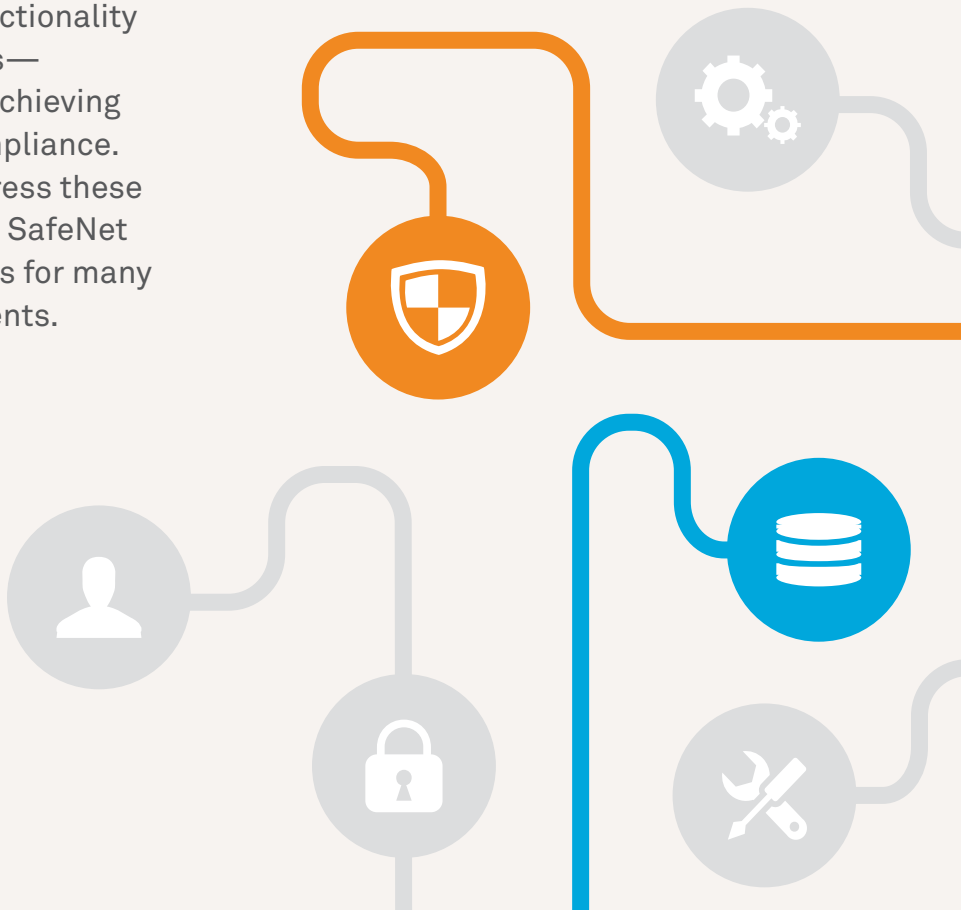
In order to protect the value of data and information to your business, that data must be completely and comprehensively secure. Whether this data is competitive information, customers' personally identifiable information, client email addresses, payment details, research, or intellectual property, the consequences of this data in the wrong hands can severely damage the reputation and performance of even the strongest organizations.

IBM's Best Practices for Data Security

IBM recommends a comprehensive approach to protecting the traditional and digital information that organizations collect and use, advocating five best practices for comprehensive data security:

1. Understand **where** your data exists
2. **Safeguard** your sensitive data
3. Look for sensitive data that exists **outside** the production environment
4. **Adapt** your security strategy as circumstances change
5. Achieve and be able to demonstrate **regulatory compliance**

In particular, SafeNet provides functionality for two of these five best practices—safeguarding sensitive data, and achieving and demonstrating regulatory compliance. In order to help organizations address these two areas, IBM has partnered with SafeNet to deliver complementary solutions for many different use cases and environments.



Data-centric Security

Effectively implementing IBM's recommended best practices requires an increasingly data-centric approach to securing sensitive information. Authentication, key management, and encryption technologies are all vital to providing persistent protection of sensitive data, access points, and user identities at all critical points in business. These technologies help organizations remain protected, compliant, and in control.

The breadth of solutions discussed in this ebook enable security teams to centrally employ defense-in-depth strategies. If access controls are lacking, the efficacy of encryption can be compromised. If identities are easily forged, your data is open to theft or sabotage. And if cryptographic keys are vulnerable, so is encrypted data.

Implementing robust access controls, strong identity management solutions, and comprehensive management capabilities will enable organizations to practically, cost-effectively, and comprehensively leverage encryption, key management, and authentication to enhance IBM's solutions and meet their security objectives. This ebook will discuss those solutions and the approaches to secure organizations' sensitive data.

SafeNet Solutions and IBM Validation Programs

The **Ready for IBM Security Intelligence** and **Ready for Cloud and Smarter Infrastructure** programs are designed to ensure compatibility between IBM products and third-party solutions. The following SafeNet products have undergone the testing and verification processes that prove close integration and have earned IBM validation:

- IBM Security Access Manager for Web/Mobile and SafeNet Authentication Solutions
- IBM Security Access Manager for Enterprise Single Sign-on and SafeNet Authentication Solutions
- IBM Security Access Manager WebSEAL and SafeNet Luna SA HSM
- IBM Security QRadar and SafeNet KeySecure
- IBM XIV Storage System and SafeNet KeySecure

The following are SafeNet-supported integrations:

- IBM PureData System for Transactions and SafeNet DataSecure and ProtectDB
- IBM Security Key Lifecycle Manager and SafeNet KeySecure and Luna SA HSM

Role of Encryption and Key Management

Encryption can be an effective approach to securing data—both when it is at rest or in transit. Experts often recommend using encryption and enterprise key management[1] to:

- Isolate regulated and sensitive information
- Separate encryption control from data center management

Deploying encryption and enterprise key management divides duties among administrators, and centralizes monitoring and audit reporting. Not only does this approach secure sensitive data, it makes demonstrating compliance and passing audits easier.

Why are encryption and key management recommended so highly? One reason is that they render the data itself useless to attackers—unlike other security measures that leave sensitive data in the clear. SafeNet's data-centric approach means that wherever the data resides, it is protected against unauthorized use and provides an additional layer of security. 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 provides 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.

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/2574918). 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.

Protecting Against Insider Threats and Nefarious Outsiders

Strong access controls are vital to being able to determine whether the individual logging in is a privileged administrator or general end user, whether they should have access to an entire system or a specific subset of elements on a given system, and so on. Systems should be able to support the concept of least privilege so that there is never a single "superuser" who can access and control all sensitive data.

Strong access controls enable security teams to understand with acuity who is trying to get access to data. When encryption is employed, one important piece of the puzzle is in place, especially when protecting against outsiders. But those keys must also be protected with strong access controls to ensure that only authorized users are able to decrypt a sensitive asset.

Basic Encryption and Key Management Principles

When encryption puts sensitive data into ciphertext, organizations tighten their control over the data by controlling decryption capabilities. If the encrypted data falls into the hands of an unauthorized user, it will have no value without the corresponding decryption key. Dividing encryption management responsibilities from the rest of the data center's maintenance adds an extra layer of data security control. As organizations enforce the separation of duties that compliance mandates require, encryption becomes a multi-pronged security tool that secures data from external and internal threats.

Database- and application-level encryption solutions allow organizations to granularly apply security policies to specific subsets of data. Encryption secures data as it progresses through workflows, and safeguards it when it is manipulated by processes running within an instance; for example, fields containing sensitive data in a web application. Yet encryption is not only for securing data at rest. It is important to also encrypt data in motion as it traverses the organization's network.

Encryption key management can present significant challenges for organizations that deploy encryption as a security tool—particularly if they have multiple, disparate deployments. Key storage, rotation, and deletion requirements can present administrative overhead and cost. 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. Largely, without a quality key management system, and as has been the trend to date, it has been difficult and uncommon for administrators to consistently adhere to the best practices around key rotation.

Basic Encryption and Key Management Principles (continued)

To improve administrative efficiency and security, organizations need centralized key management solutions that offer the highest level of protection, and that streamline such activities as key rotation and deletion. Finally, organizations should look to work with solutions that adhere to NIST 800-57 key management guidelines and support the OASIS Key Management Interoperability Protocol (KMIP). These standards offer flexibility and broad interoperability, enabling organizations to begin to centralize the management of cryptographic keys across disparate encryption deployments, which yields benefits in security, administrative efficiency, and compliance.

In addition, key management best practices require a secure root of trust to store keys. For applications and data that are subject to rigorous contractual or regulatory requirements, high-level protection in tamper-proof appliances is often necessary. For the entire security infrastructure to be secure and above reproach, administrators need to trust the integrity of the encryption material protecting the data.

Remaining agile while mitigating risk

Virtualization and cloud-based services make it likely that organizations have their data—including sensitive data—in many places. When circumstances change—and with cloud-based services, that may be a frequent occurrence—it's essential to implement a security approach that can adapt to many environments. "Business leaders need to begin to formulate a strategy that brings security controls closer to data so they can ensure it remains protected," explains Leonor Martins, a virtualization and cloud solutions specialist with SafeNet.

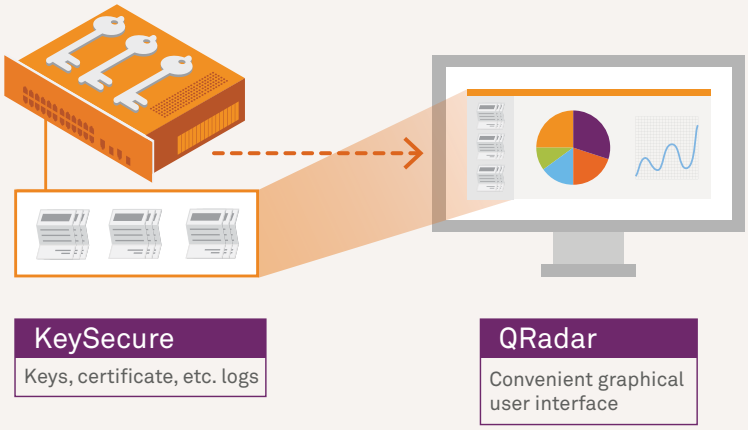
Data-centric security does not rely on a perimeter to hold fast in order to keep the data secure. With encryption and proper management of those encryption keys, the data can live anywhere.

IBM QRadar Security Intelligence Platform and SafeNet KeySecure

IBM® QRadar® Security Intelligence Platform integrates SafeNet KeySecure's encryption key logs into its Security Information and Events Management (SIEM) system. QRadar organizes millions of data points from network security events and reduces thousands of daily security alerts into a manageable list of actionable security insights worthy of further investigation. In KeySecure managed environments, administrators can consolidate key data and visualize key logs in a convenient Graphical User Interface (GUI) for closer, comprehensive monitoring of the enterprise key management infrastructure.

KeySecure is an encryption and key management appliance that centralizes the control of an enterprise's disparate encryption solutions. By consolidating the policy and key management of application servers, databases, and file servers it streamlines security administration. 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. Additionally, unifying and centralizing policy management, logging, and auditing makes compliance information more readily accessible for QRadar to pull into its out-of-the-box preconfigured reports.

KeySecure gives organizations the security and administrative advantages of centralized key management, while QRadar unlocks additional value from KeySecure's tracking features and improves overall vulnerability protection.

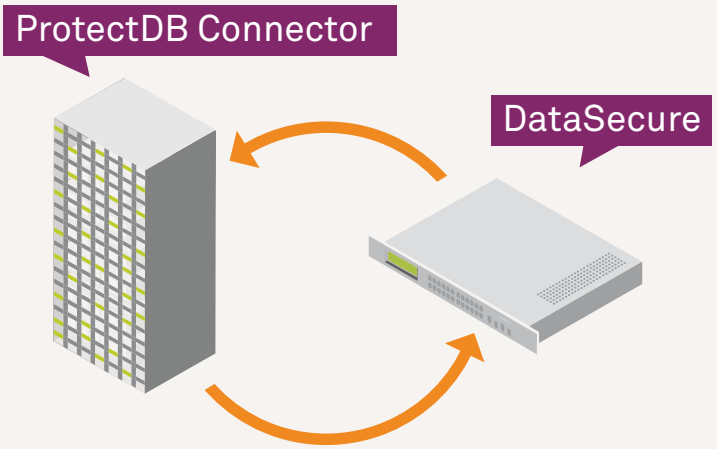


Business Partner IBM
Ready for
Security Intelligence

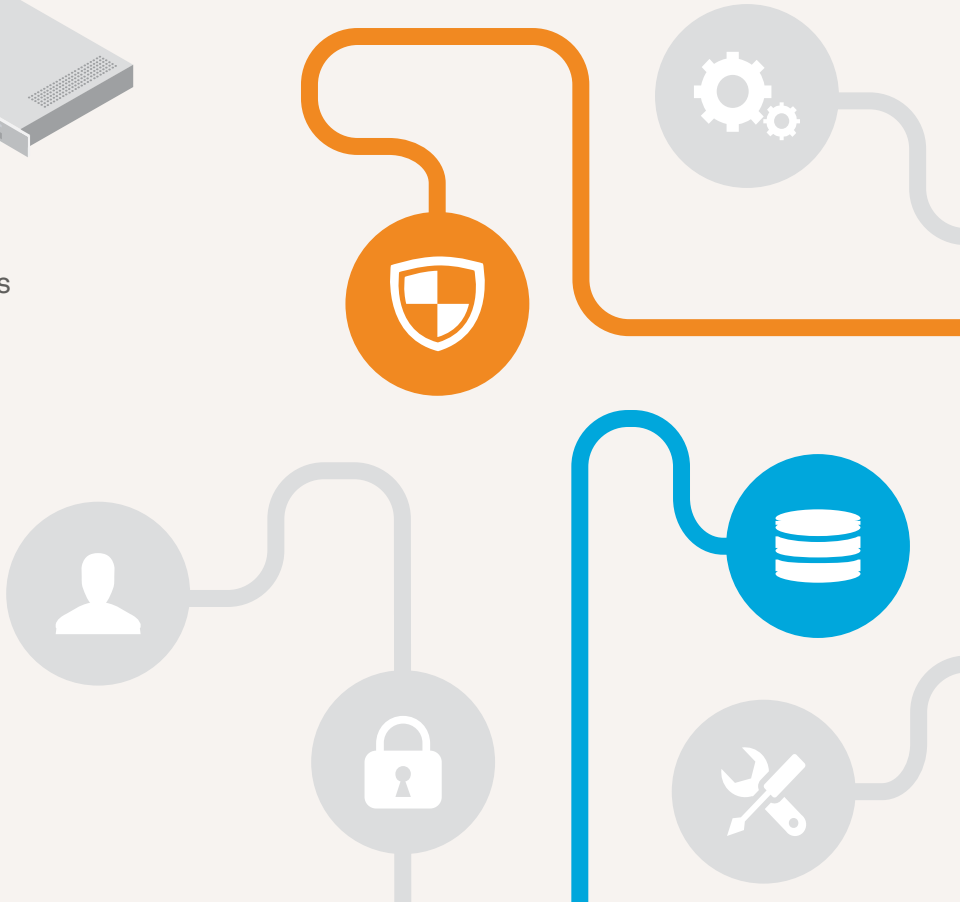
IBM PureData System for Transactions and SafeNet DataSecure and ProtectDB

IBM PureData System for Transactions, powered by IBM's DB2® database software, is a fully integrated system optimized for delivering highly scalable transactional workloads. Capable of consolidating more than one hundred databases on a single system, its active clusters ensure reliable data availability as systems scale. SafeNet DataSecure and ProtectDB deliver powerful database encryption and centralized key management to secure sensitive data automatically as it flows into and out of PureData System for Transactions databases. Encryption takes place at the column level, altering existing tables to store the resulting ciphertext so customers benefit from security without losing important database functions.

DataSecure with ProtectDB provides a fast, flexible, and seamless solution to address business needs and compliance requirements. IBM PureData System for Transactions provides highly scalable and highly reliable data services, ready in minutes, which SafeNet secures—making it an ideal combination for mission-critical enterprise applications.



PureData System for Transactions



SafeNet. THE DATA PROTECTION COMPANY

IBM XIV Storage System and SafeNet KeySecure

IBM XIV® is a high-end disk storage system whose easy provisioning, autonomic data placement, and GUI make it ideal for the cloud. Additionally, XIV storage offers elastic scaling with IBM Hyper-Scale, and robust data security through encryption of data at rest. Using the OASIS KMIP standard, KeySecure integrates with XIV storage for secure, centralized encryption key management.

In addition to managing keys for XIV storage, KeySecure unifies the management of cryptographic materials for a variety of encryption products, including self-encrypting drives, tape archives, Storage Area Networks, virtual workloads, applications, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard. Having a central appliance from which to administer keys simplifies the management of the encryption infrastructure across the entire key lifecycle, including secure key generation, storage and backup, key distribution, deactivation, and deletion. KeySecure streamlines and secures administration by making automated, policy-driven operations easy, and by ensuring administrators are restricted to roles appropriate for their scope of responsibilities.

The value of KMIP

The Key Management Interoperability Protocol (KMIP) standardizes communication between enterprise key management systems and encryption systems in order to reduce the time and costs required to manage encryption keys from disparate encryption deployments scattered across locations and workgroups. The protocol allows heterogeneous cryptographic environments and key managers to communicate without custom integration. It reduces not only the operational costs for enterprise key management but also the time and effort involved in the integration.

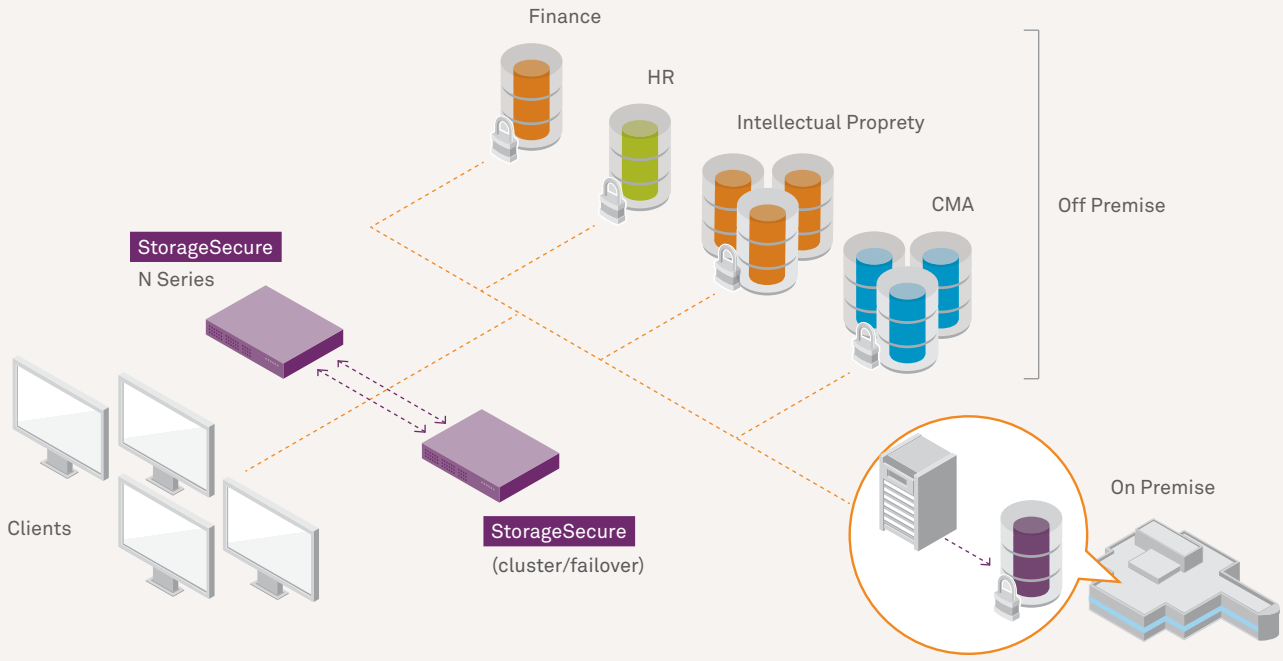
Any KMIP supporting environment—self-encrypting hard drives, tape drives, databases, applications, and encryption SDKs—can use the protocol to communicate with any compliant key manager. Today, customers benefit from a large ecosystem of KMIP-compliant solutions produced by IBM, NetApp, Hitachi Data Systems, HP, Sepaton, CipherCloud, and others. For more information on SafeNet's KMIP interoperability, click **here**.

IBM N Series NAS Storage and SafeNet StorageSecure

SafeNet provides advanced encryption services based on high-speed, 256-bit AES encryption for IBM NAS-based storage solutions. IBM N Series users continue to enjoy the clustered Data ONTAP® operating system's unique features while adding robust data security afforded by SafeNet StorageSecure encryption and SafeNet KeySecure enterprise key management.

Clustered Data ONTAP gives IBM N Series storage users efficiency technologies such as Snapshot copies; thin provisioning; FlexClone®, SnapMirror, and SnapVault® technologies; and RAID-DP® technology. StorageSecure, a self-contained encryption appliance, delivers 256-bit AES encryption to secure data stored in Ethernet-based (NAS file servers or iSCSI LUNs) storage environments. Additionally, with StorageSecure you can add layers of access control to strengthen existing LDAP, MS AD, and NIS controls, secure data for compliance mandates and protect offline archived data from unauthorized access or theft.

This combination of a modern storage infrastructure and SafeNet security appliances delivers the peace of mind that your data is protected against unauthorized access while simultaneously making the most efficient use of your storage investments.



Roots of Trust

Roots of trust, as defined by the Cryptographic Technology Group at the US National Institute of Standards and Technology (NIST)[1], are components that are inherently trusted to perform one or more security-critical functions. Protecting cryptographic keys, performing device authentication, or verifying software are three examples.

These components must be secure by design and, according to NIST, are ideally implemented in or protected by tamper-resistant hardware.

Keys in Hardware vs. Software

When cryptographic keys are stored on the same server as the other components of a system, it is much easier to gain access to those keys and compromise that system. This is a major weakness of encryption solutions that store cryptographic keys in software. Hardware security modules (HSMs) are designed to create a barrier between software on the server and cryptographic key material. HSMs achieve this by offloading cryptographic keys from an application server and isolating them in dedicated hardware. This approach greatly mitigates the attack vector for a hacker seeking to access sensitive cryptographic keys.

1 http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf

IBM Security Access Manager WebSEAL and SafeNet Luna SA HSM

IBM and SafeNet, via IBM Security Access Manager WebSEAL and Luna SA HSM, deliver integrated capabilities that enable customers to optimize the security and performance of online communications and transactions. Together, enterprises can harness secure key and certificate storage and robust SSL acceleration to protect their online presence and business applications, along with transactions.

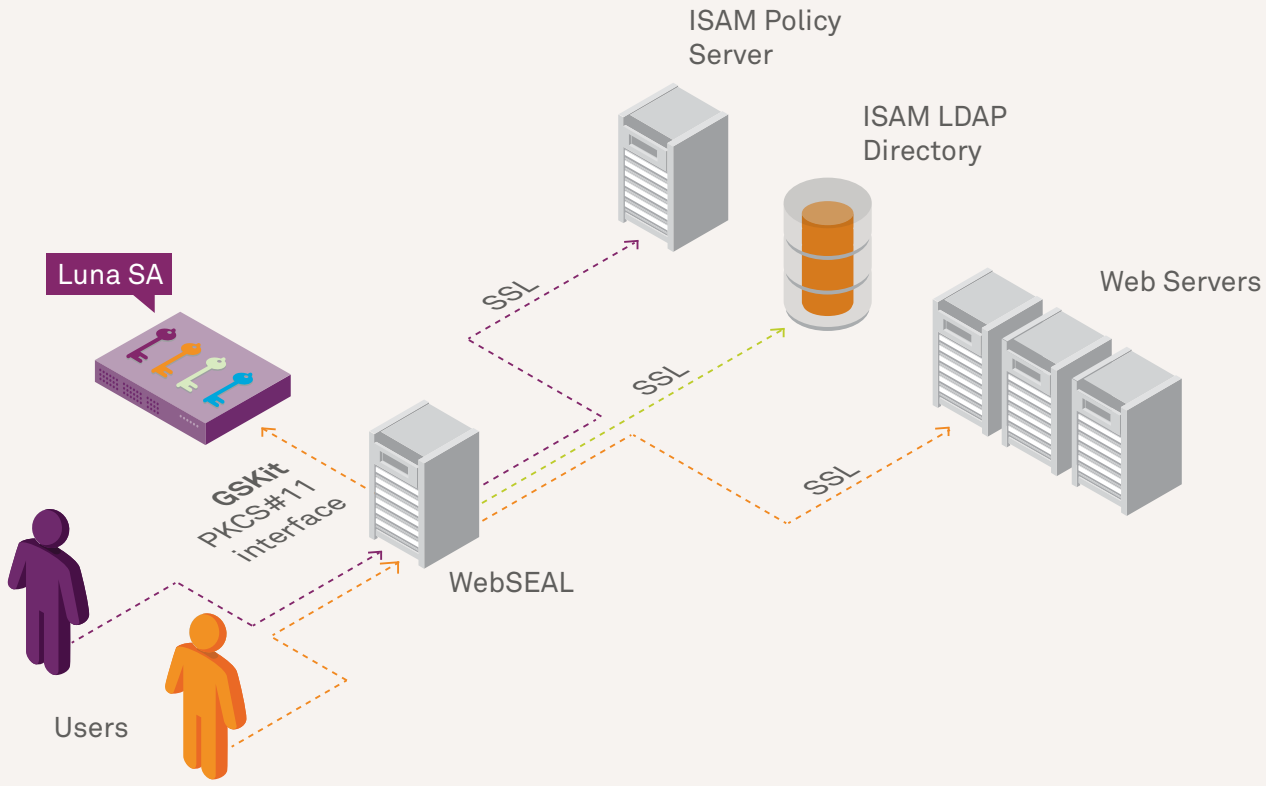
IBM Security Access Manager WebSEAL is a high-performance web server that allows customers to apply fine-grained security policies to their web-based Security Access Manager environments. WebSEAL provides single sign-on capabilities and enables customers to apply policies to back-end web application server resources. Using IBM Global Security Kit (GSKit) libraries, ISAM WebSEAL uses encryption to secure network communications. To maintain the integrity of SSL operations, ISAM WebSEAL stores encryption keys at the root of the SSL handshake in Luna SA HSMs.

Luna custom integration

Luna SA can integrate with hundreds of third-party products, and with a large number of cryptographic protocols and APIs, such as PKCS#11, CAPI (Microsoft CryptoAPI 2.0), CNG (Microsoft Cryptography API: Next Generation), JCA (Java Cryptographic Architecture), and OpenSSL. For specifics on integration, visit SafeNet's HSM interoperability page.

IBM Security Access Manager WebSEAL and SafeNet Luna SA HSM (continued)

Luna SA HSMs are robust, high-availability, high-performance appliances that ensure the integrity of cryptographic operations. Its FIPS 140-2 Level 3 tamper-proof 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, Luna SA HSMs are capable of performing thousands of cryptographic transactions per second, offering the throughput and responsiveness to support the most demanding SSL applications.

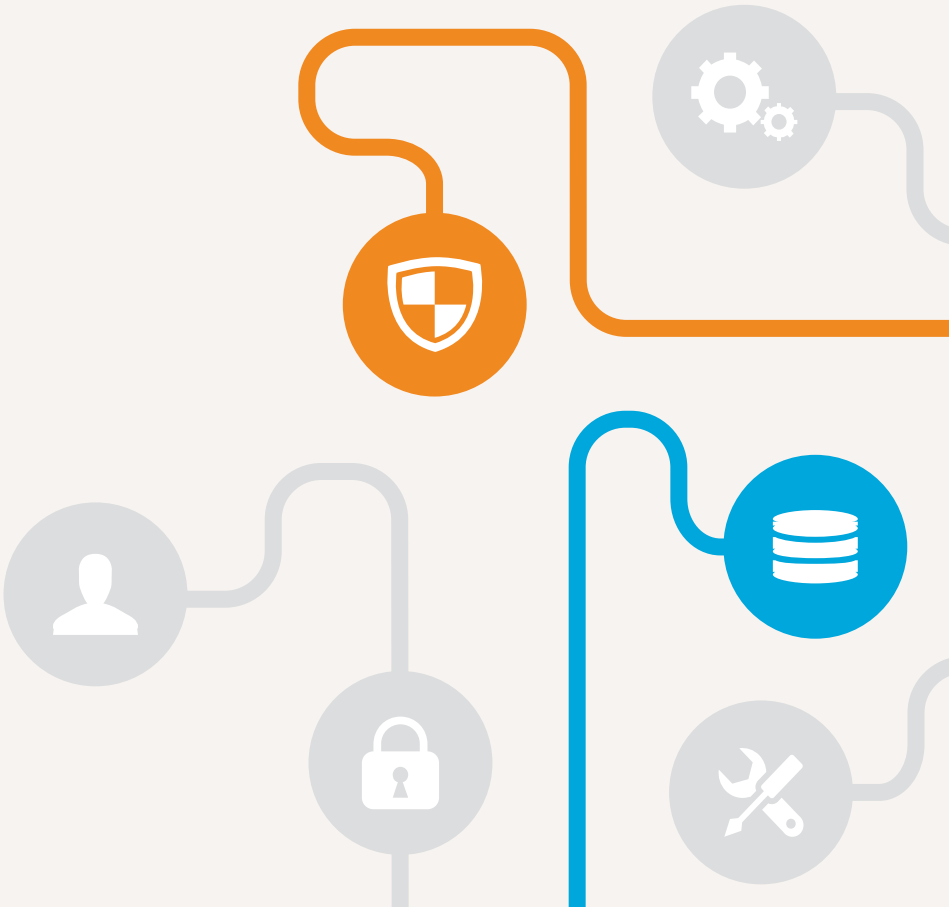


IBM Security Key Lifecycle Manager and SafeNet Luna SA HSM

IBM® Security Key Lifecycle Manager—formerly Tivoli Key Lifecycle Manager—is a hardware appliance that centralizes and simplifies encryption and key management processes. It offers key lifecycle management for both IBM and non-IBM storage devices. While the key manager simplifies processes, it cannot provide key storage security on its own. SafeNet Luna SA integrates to securely store encryption keys in a tamper-proof hardware security module.

IBM Security Key Lifecycle Manager, when backed by Luna SA HSMs, helps organizations comply with such mandates and regulations as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), and the Health Insurance Portability and Accountability Act (HIPAA). Luna SA's FIPS 140-2 Level 3 validation is the perfect solution for Security Key Lifecycle Manager controlled environments that need to comply with strict standards and regulations.

Business Partner IBM
Ready for Security Intelligence

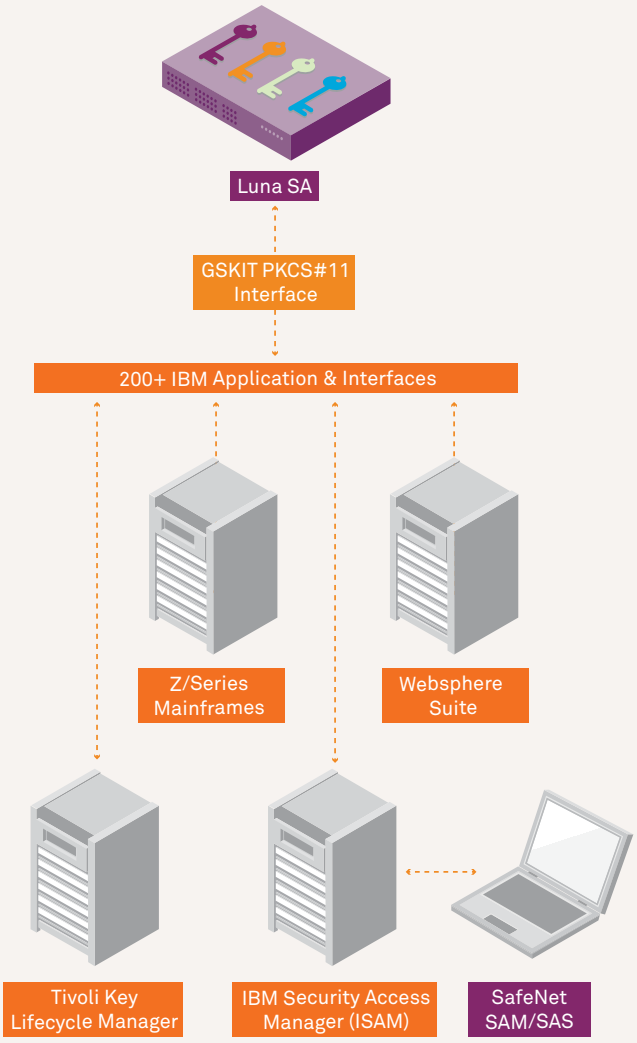


SafeNet. THE DATA PROTECTION COMPANY

IBM Global Security Kit (GSKit) and SafeNet Luna SA HSM

GSKit provides libraries and utilities for SSL communication, enabling organizations to add encryption protection to over 200 IBM applications, including the IBM WebSphere Suite and IBM Security Access Manager (ISAM). Businesses stand to lose substantially – both in revenue and reputation – when there is a breach of online channels they use for communication, transactions, and applications. SSL encryption secures these web based communications and services. Luna SA stores SSL certificates in a tamper-proof hardware security module to serve as a reliable root of trust for network cryptographic operations.

Additionally, Luna SA offloads SSL operations from general-use servers, stores them within the hardware appliance for added security, and improves server performance. It can also provide true random number generation and streamline key administration by performing both symmetric and asymmetric key functions on a single platform. Together, IBM and SafeNet optimize the security and performance of online communications and transactions.



The value of multi-factor authentication

With advances in technology that allow decentralized users to access enterprise resources for increased productivity and lower costs comes the question: How do organizations know that users are representing themselves honestly? Lost or stolen credentials can pose significant security risks as resources, and access to those resources, move beyond the traditional data center. Technological advances have made delivering applications from or storing data in remote sites cheap and easy. Each time a resource is moved beyond the traditional data center, a password becomes required. 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 can increase their confidence that users are correctly identified by deploying multi-factor authentication. These solutions add an extra layer of identity verification to ensure that users are who they represent themselves to be. This verification requires an exchange of material or information that only the appropriate user would know. Unique, assigned security certificates, extra passwords, biometric information, or randomly generated number passwords valid for a single use can be used in varying forms to confirm, with a high degree of confidence, a user's identity. 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.

Organizations can deploy multi-factor authentication in a variety of ways. Physical tokens and smart cards can be easy and convenient, while cloud-based authentication-as-a-service models are flexible, economical alternatives adapted to trends in user mobility. Hidden behind the token or the one-time password is a platform that can improve the way administrators deploy and manage their authentication infrastructure. Policy-based controls, automation, and integration with existing directories are features that administrators can use to reduce risks while preserving a positive user experience.

SafeNet's authentication solutions integrate with a number of IBM products to ensure that only authorized users gain access to their enterprise's valuable resources.

ISAM for Web/Mobile and SafeNet Authentication Solutions

IBM Security Access Manager and SafeNet strong authentication form a solution that streamlines entry to online corporate resources, and helps organizations protect valuable information by hardening access to those resources, eliminating the use of simple passwords, which can be easily stolen or hacked. Validated through the Ready for IBM Security Intelligence program, the solution features close integration so customers can expect smooth integration, configuration, and management.

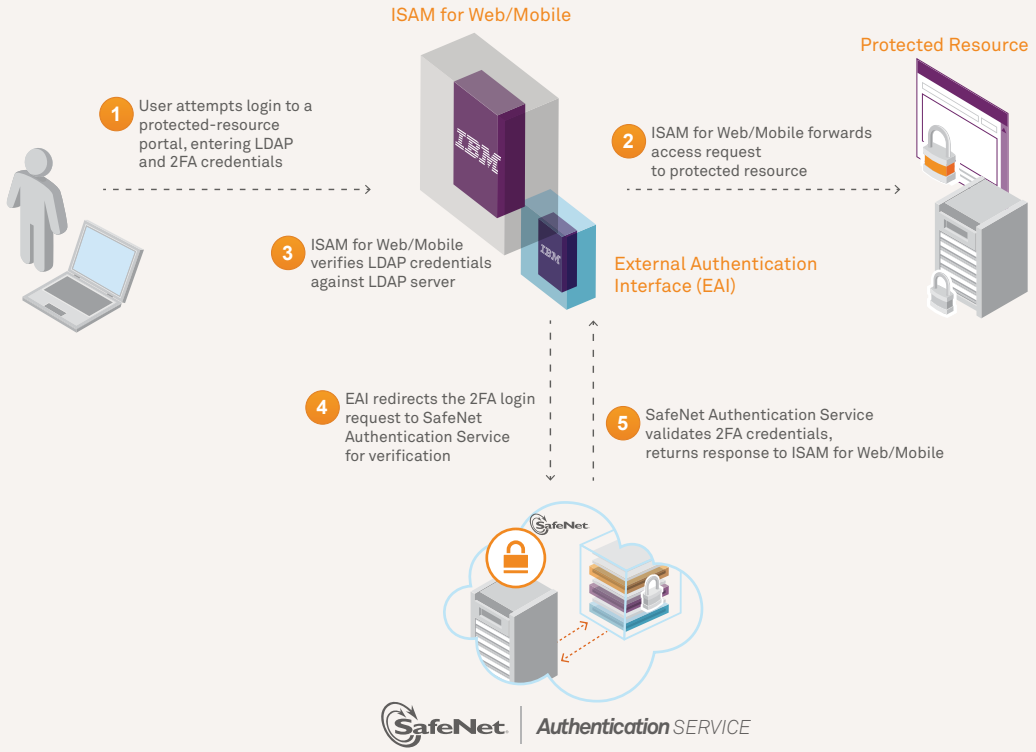
IBM Security Access Manager (ISAM) for Web provides an integrated security management platform for authentication and authorization services, access control, web single sign-on (SSO), and auditing across an enterprise's resources. Its integrated, policy-based security setup manages employees and external users (e.g., customers, business partners, suppliers, distributors, etc.) so they can securely access enterprise resources while limiting the number of passwords vulnerable to compromise.

SafeNet's strong authentication adds an extra layer of identity protection to ISAM for Web/Mobile that reduces the risk of unauthorized access from identity theft. Organizations can securely offer their employees or external users' access to web applications protected behind the ISAM/SAS solution. SafeNet offers a wide range of authentication methods and form factors, including context-based authentication, certificate-based authentication, OTP, and out-of-band. These are enabled with SafeNet Authentication Service, a cloud-based authentication service, and SafeNet Authentication Client, middleware that supports certificate-based authentication.

SafeNet Authentication Service (SAS)

SafeNet Authentication Service (SAS) delivers fully automated, highly secure, cloud-based authentication-as-a-service for enterprises and service providers. With support for a wide range of authentication methods, SafeNet Authentication Service protects a broad IT ecosystem, including SaaS applications, VDI, 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 environments easy and painless.

OTP Authentication with ISAM for Web/Mobile using SafeNet Authentication Service



Strong Authentication with ISAM for Web/Mobile using SafeNet Certificate-based Tokens

IBM Security Access Manager for Enterprise Single Sign-on (eSSO)

IBM Security Access Manager for Enterprise Single Sign-on (eSSO) uses SafeNet authentication solutions to provide ISAM eSSO users with strong authentication for both personal and shared workstation configurations. Users can log on, lock, and unlock ISAM eSSO's AccessAgent only by using a smart card or PIN. Through the SafeNet Authentication Client, a unified middleware client, organizations can take advantage of SafeNet's extensive portfolio of certificate-based authenticators—including eToken and iKey smart card, USB, and software-based devices—for their strong authentication needs.

Security Access Manager for Enterprise Single Sign-On provides users with a single point of entry for Microsoft Windows, web, Java, and mainframe applications from such endpoints as laptops, virtual desktops, servers, or web portals. Regardless of the endpoint or location, users can access important enterprise resources via ISAM eSSO. For the organization, ISAM eSSO reduces costs by automating administrative tasks such as password resets, strengthens security by eliminating multiple passwords in favor of a single multi-factor authentication solution, and improves productivity by ensuring that authorized users have access when they need it.

With this two-factor authentication solution, organizations can easily and effectively expand business opportunities by providing secure network access, improve data security through enhanced encryption and digital signing, and reduce costs and vulnerabilities through superior password management.

For more information

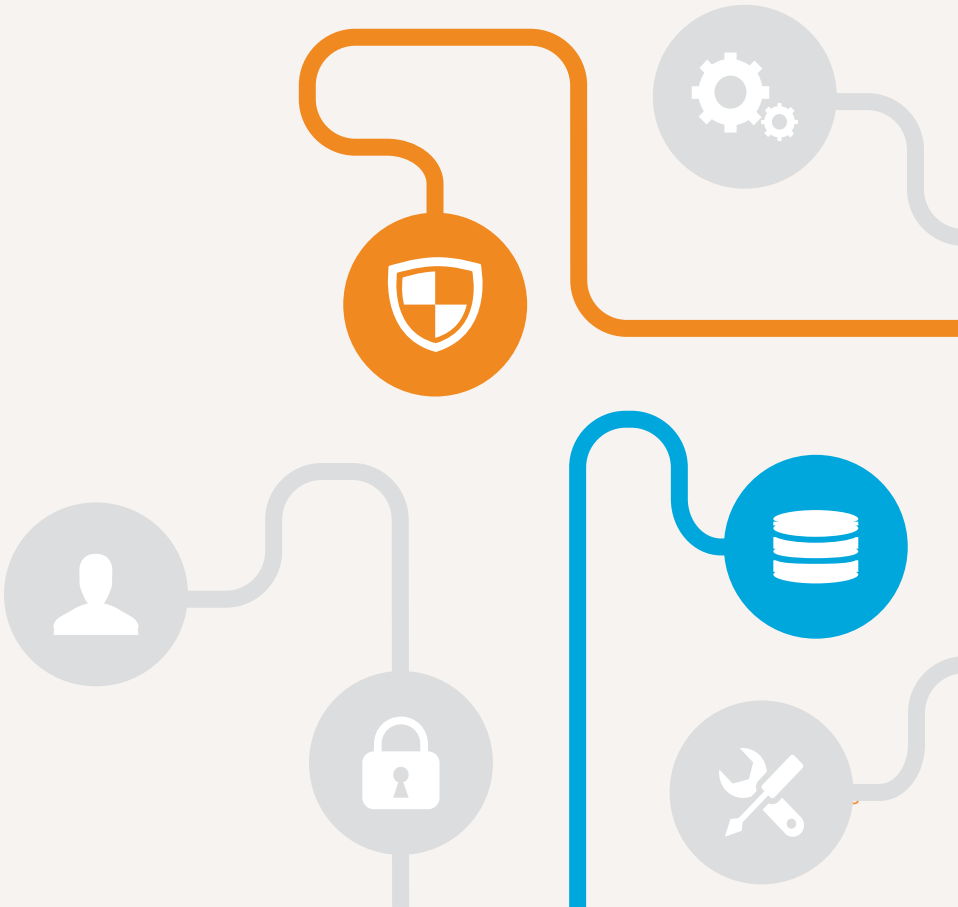
Helping to protect the confidentiality, integrity, and availability of customers' systems and data is of the utmost importance to IBM, as is maintaining customer trust and confidence.

SafeNet, a leading global provider of data protection, has many solutions that are verified by IBM, a Platinum-level SafeNet Cipher Technology Partner. For over 30 years, SafeNet has been securing and protecting the valuable data assets and intellectual property of Fortune 500 global corporations, government agencies, and other organizations.

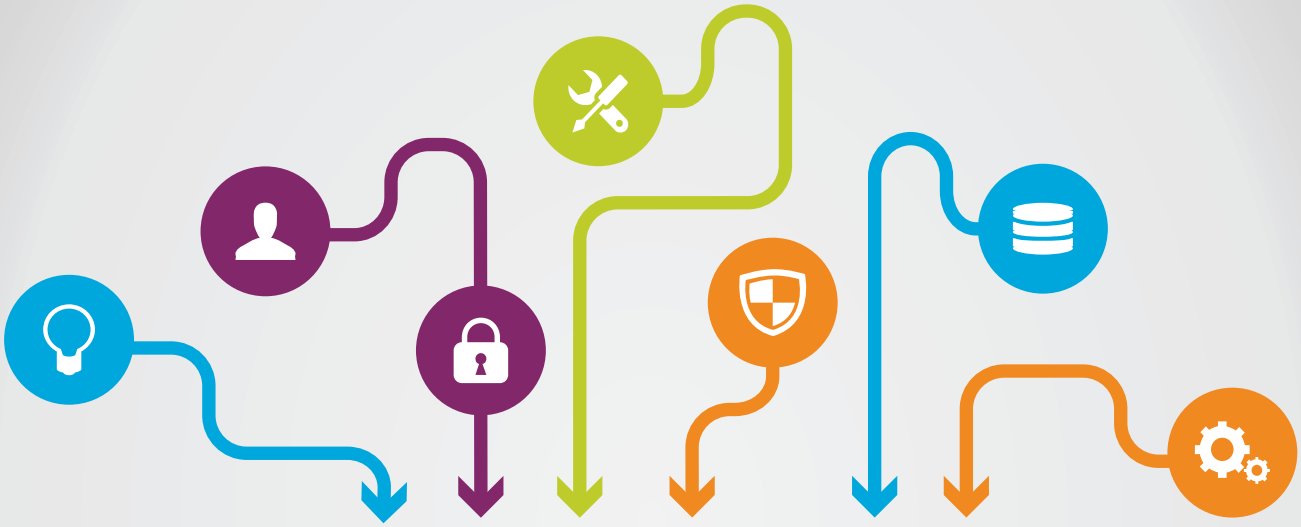
SafeNet's data-centric approach for sensitive information focuses on the protection of high-value information throughout its lifecycle. Thousands of customers trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

For more information regarding IBM and SafeNet integrations, visit **http://www.safenet-inc.com/partners/ibm.**

To visit SafeNet's IBM DeveloperWorks community, go to **https://ibm.biz/BdRmhf.**



SafeNet. THE DATA PROTECTION COMPANY



SafeNet

THE
DATA
PROTECTION
COMPANY

SafeNet security enhancements for **IBM solutions**

June 2014, Version 1