THALES

www.thales-esecurity.com

NEXT-GENERATION DATA-AT-REST SECURITY FOR BIG DATA AND CLOUD APPLICATIONS

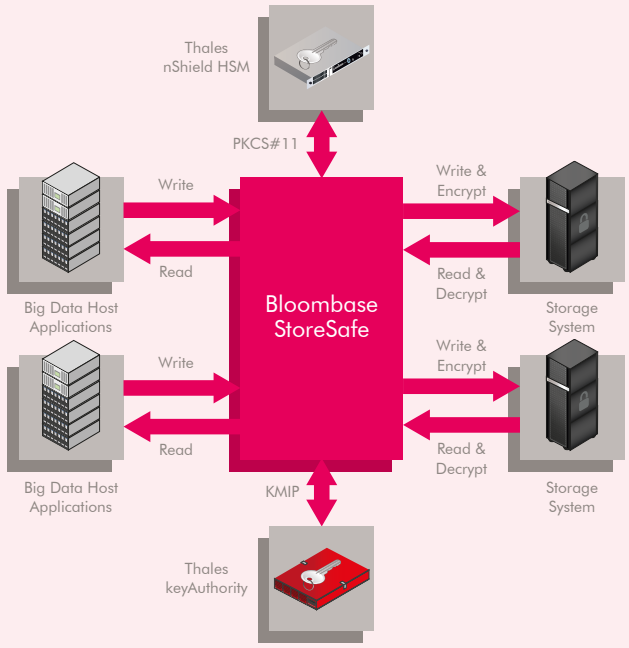
Solution Benefits

- Protects sensitive data at rest no matter where it resides
- Enables transparent encryption for business software applications
- Provides a FIPS 140-2 Level 3 platform for cryptographic acceleration and key management
- Scales from physical and virtual on-premises data center to cloud-based environments
- Facilitates compliance with data privacy and security regulations

BLOOMBASE®

Thales e-Security

Bloombase and Thales Deliver Storage Encryption Solution for Security Compliance



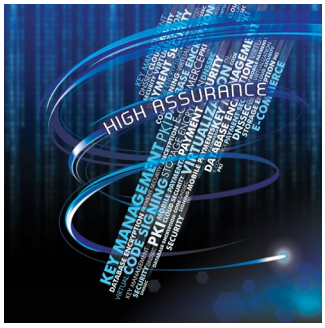
Thales nShield Connect and keyAuthority integrate with Bloombase StoreSafe to enhance cryptographic capabilities and to facilitate compliance with regulatory requirements.

The Problem: Need to protect an increasing volume of security-sensitive data in storage

Organizations capture and store increasing volumes of data, including private and sensitive data, for advanced analytics and business intelligence purposes. This trend, combined with the growing volume of sensitive data generated by smart devices in the new Internet of things (IoT), makes data storage infrastructure a prime target for attack. Encryption protects data privacy, however the techniques used to encrypt data can vary among business applications. With diverse applications deployed across an increasingly decentralized environment, effectively protecting the growing volume of sensitive data is critical to ensure the security of these systems.

The Challenge: Securing complex heterogeneous data storage environments with a comprehensive encryption solution

Enterprises are migrating from on-premises to cloud-based storage services to better manage increasing data volumes. The trend has been accompanied by a shift from selective encryption of data classified as sensitive, to a policy that encrypts everything in storage. The degree to which organizations can trust this approach depends directly on the protection of cryptographic keys. Encryption keys underpin security, and safeguarding and managing them is critically important. As more data gets encrypted, more keys need to be secured and managed to protect data in storage and to ensure it can be decrypted when needed.



BLOOMBASE AND THALES DELIVER STORAGE ENCRYPTION SOLUTION FOR SECURITY COMPLIANCE

The Solution: Bloombase and Thales together deliver high performance and enhanced security to heterogeneous storage infrastructures

Bloombase StoreSafe is an agentless software-appliance encryption solution for data at rest applications. Its application-transparent and protocol-preserving features enable it to protect the entire spectrum of storage infrastructures from on-premises, to virtualized, and big data cloud-based storage services. Bloombase StoreSafe operates as a storage proxy, transparently encrypting data before it is physically stored. Decryption is performed on the fly as data is requested from storage by the application. The schema guarantees operational transparency and maximum interoperability, while ensuring that unauthorized clients cannot access decrypted data.

Bloombase customers can leverage trusted cryptography solutions from Thales to facilitate compliance with regulatory requirements. Depending on the deployment environment, customers can integrate Bloombase StoreSafe with either the Thales nShield Connect hardware security module (HSM) or with the Thales keyAuthority centralized key manager. These devices provide a FIPS 140-2 Level 3 environment for protecting and managing critical cryptographic keys and enable compliance with regulatory requirements for public sector, financial services, and large enterprises.

When to use nShield Connect?

Deployments using a storage security application that seek to offload cryptographic capabilities to a dedicated hardware appliance can use Thales nShield Connect. The HSM is typically deployed in the data center alongside the Bloombase StoreSafe encryption solution. Thales nShield Connect delivers low latency hardware-accelerated encryption and key management services for traditional enterprise data storage and archival applications.

When to use keyAuthority?

Deployments using diverse storage security applications that seek to externalize key management use Thales keyAuthority. The centralized key manager interfaces with multiple storage security applications using an industry-standard protocol (KMIP). keyAuthority scales to protect millions of keys, provides enterprise-wide enforcement of encryption controls, and partitions users and keys for compliance with mixed security policies.

Thales

Thales nShield Connect delivers high performance cryptographic services for mission critical storage security applications. The network-attached HSM:

- Provides a FIPS 140-2 Level 3 certified, tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Performs encryption/decryption on behalf of the storage security applications
- Interfaces with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

Thales keyAuthority offers best-in-class centralized key management services for storage security applications. The market-leading key manager appliance:

- Safeguards and manages encryption keys in a FIPS 140-2 Level 3 designed, tamper resistant chassis external to the storage security applications
- Provides enterprise-wide key management services for diverse storage security applications
- Interfaces with applications using an industry-standard key management protocol (OASIS KMIP)

Bloombase

Bloombase StoreSafe delivers turnkey, non-disruptive, encryption for data at rest. The purpose built scalable architecture:

- Protects both on and off-premises at-rest data systems from SAN, NAS, DAS, tape library to virtual tape library (VTL), regardless of the complexity of the heterogeneous storage infrastructure or medium
- Secures data in content addressable storage (CAS), object stores, virtual hypervisor datastores, and RESTful cloud storage service endpoints
- Enables enterprises to mitigate data leakage threats

For more detailed technical specifications, please visit www.thales-esecurity.com or www.bloombase.com

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com