Zettaset

SOLUTION BRIEF

Zettaset Big Data Encryption Key Management

V-EKM Virtual Enterprise Key Manager
V-HSM Virtual Hardware Security Module
S3 Basic Client

Data-Centric Security Optimized for Big Data and Cloud

The demand for encryption continues to increase as data breaches become more frequent and disruptive. The soaring costs associated with data breaches include lost business, customer notifications, legal services, and brand damage. Encryption mitigates these risks and is one of the most proven defenses against data breaches and by protecting the data itself. Encryption also helps companies to comply with corporate and government regulations for data security and privacy.

The Zettaset Big Data Encryption Suite™ provides data-centric security utilizing advanced encryption technologies to ensure the highest levels of protection for critical data in the cloud and on-premises. The Zettaset Big Data Encryption Suite has been designed from the ground up for optimal performance and scalability in distributed Big Data systems like Hadoop and NoSQL, as well as the latest generation of Relational databases.

> *"The only way to secure databases on virtual machines or in cloud environments, without sacrificing the huge benefits of these new architectures, is to use software-based solutions that share the elasticity of virtual machines and cloud computing."*

Organizations are increasingly adopting the cloud for data management to benefit from lower operational overhead and infrastructure costs as well as flexible storage capacity options. The only way to secure databases on virtual machines or in cloud environments, without sacrificing the huge benefits of these new architectures, is to use software-based solutions that share the elasticity of virtual machines and cloud computing.

All Software-Based Approach to Encryption and Key Management for Greater Operational Efficiency and Flexible Deployment

Zettaset delivers a software based encryption solution that can readily match the elasticity of virtual machines and cloud computing. As virtual machines running the database are provisioned (and de-provisioned) to balance capacity needs, no manual intervention is required at the management console. Deploying software-based key managers and HSMs is more cost-effective and less disruptive than traditional hardware approaches in highly elastic cloud environments, offering power users greater operational efficiencies.

Solution Highlights

- All software solution reduces hardware costs associated with traditional key managers and HSMs, simplifies encryption deployment and security operations, ideal for elastic cloud environments where resources must be provisioned and de-provisioned on-demand
- Addresses critical gaps in Hadoop / NoSQL open-source ecosystems with a commercial, monetizable solution that provides greater data protection, enterprise integration, and ease of use
- Zettaset S3 Basic Client enables organizations to take total control of key access while using cloud services, making it unnecessary to provide CSPs with key access
- Zettaset compliance with KMIP and PKCS#11 standards eases integration into existing key management, hardware security module, and encryption systems environments, enabling customers to retain the value of their existing technology investments
- Advanced big data encryption solution is optimized for scalability and performance in distributed computing architectures and elastic cloud environments

The Zettaset Big Data Encryption Suite includes a virtual enterprise key manager, HSM, and encryption software that can be easily added to a virtual machine or cloud when and where needed.

- Zettaset V-EKM™ (Virtual Enterprise Key Manager) is a software-based key manager that automates the management and control of policies that protect and control access to business-critical encryption keys.
- Zettaset V-HSM™ (Virtual Hardware Security Module) is a software-based HSM that securely stores the master key and master hash key used to encrypt and hash the contents of the key manager database.
- Zettaset encryption systems software includes BDEncrypt™ for high-performance disk encryption, and BDEncrypt Plus™ for file-level encryption plus data integrity protection against unauthorized data manipulation.

Zettaset enables organizations to efficiently and securely manage and store cryptographic keys and policies throughout the key management lifecycle in the enterprise. Zettaset can deliver layered encryption for file, zone, directory and partition levels, depending on the granularity requirements of the data environment. Key management and encryption can be applied to Hadoop, NoSQL and Relational databases, as well as multiple file and object storage systems.

Every component of the Zettaset Big Data Encryption Suite is fully-compatible with existing Key Management Interoperability Protocol (KMIP) key managers and Public Key Cryptography Standard (PKCS) #11 hardware security module (HSMs), and therefore can fit into any customer environment where these products already exist. The Zettaset V-EKM virtual enterprise key manager keeps a database of encryption keys which are encrypted and protected using master keys in HSMs. The master keys are accessed through a PKCS#11-standard interface.

Zettaset V-EKM Virtual Enterprise Key Manager Features and Benefits

- Software-based encryption key management reduces hardware requirements, simplifies encryption deployment and on-going administration
- Optimized for scalability and performance in dynamic Big Data distributed computing distributed systems in the cloud, or on-premises
- Full key life-cycle support including key erasure, backup and restore
- KMIP and PKCS#11 compliant - Can be used as part of any KMIP and PKCS#11-compliant solution
- File metadata cryptographically protected and tied to data for complete file protection
- Highly automated management

Zettaset V-HSM Hardware Security Module Features and Benefits

- Software-based hardware security module (HSM) reduces hardware requirements, simplifies encryption deployment and on-going administration
- Securely stores keys and hash keys used to encrypt and hash contents of key manager database, enabling a caller to do crypto operations with keys while securely retaining them within the HSM process
- Supports secure key exchange between HSMs to create backup HSMs for redundancy
- Optimized for scalability and performance in dynamic Big Data distributed computing distributed systems in the cloud, or on-premises
- Light weight, self-contained solution runs on UNIX OS
- PKCS#11 compliant - Can be used as part of any PKCS#11 compliant solution

Customer-Controlled Encryption with Zettaset S3 Basic Client

Migrating data to the cloud and third-party CSPs provides organizations with operational advantages, but may also create unwanted exposure. Some CSPs require that their customers provide them with encryption key access. For many organizations, providing a third-party with encryption key access poses a significant risk in the form of compliance violation, compromised privacy, and reduced overall data security.

Therefore, it is of paramount importance that encryption keys are owned and managed solely by the owner of the data. Being the sole owner of the encryption keys for your company's data in the cloud means that it cannot be accessed by any unauthorized person, company, government, or business entity that does not

> *"Encryption is one of the best ways to secure corporate data in the cloud, but it has to be encryption that the company controls."*
>
> *- Forrester Research, Jonathan Penn*

hold the encryption key. Responses to data access requests can be answered only by the key owner, because they are not in the hands of a third-party.

Zettaset S3 Basic Client enables organizations to take total control of key access while using cloud services, making it unnecessary to provide CSPs with key access.

Zettaset S3 Basic Client Features

- One key per S3 bucket
- Manual key generation by the administrator
- Highly efficient and secure AES GCM crypto from the client
- Java API and command line management support
- Utilizes the Zettaset V-EKM Virtual Enterprise Key Manager and V-HSM hardware security module

Benefits of Total Control of Encryption Key Access to Encrypted Cloud Data

Zettaset S3 Basic Client provides customers with the following benefits of total encryption key control.

- As the sole key owner, you address any and all access requests for the surrender of your company's encrypted data.
- You manage the encryption key lifecycle and storage, enabling you to demonstrate compliance and ensure that your cloud data is always secure.
- You define and control data access permissions for company personnel, partners, vendors, customers, etc., to prevent unauthorized access to your cloud data.
- Third-parties cannot access the encryption key or gain access to your data through the CSP unless permitted by you.
- You are the only entity with access to data because you own the data encryption and the encryption keys.

Enterprise-Wide Interoperability and Systems Fit

The Key Management Interoperability Protocol (KMIP) and Public Key Cryptography Standard #11 (PKCS) are specifications developed by OASIS that standardize communication between enterprise key management systems, hardware security modules, and encryption systems. OASIS (Organization for the

Advancement of Structured Information Standards) is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.

Every component of the Zettaset Big Data Encryption solution adheres to these standards, to ensure interoperability with other standards-based key management systems, hardware security modules, and encryption systems that may exist within the enterprise and the cloud.

Certified partners include:

gemalto security to be free

Hewlett Packard Enterprise

THALES

utimaco®