

Software-defined Encryption for NetApp StorageGRID

The Challenge

Object storage is the storage system of choice for leading Cloud Service Providers, and NetApp is a leading provider of object storage. Whether the storage location is on-premises or in the cloud, encrypting sensitive data continues to be a requirement for regulatory compliance and mandated corporate policies. But encrypting data in the cloud creates a new security challenge. Who should control the cryptographic process and the management of the encryption keys – server side or client side? Client side is preferred, as the user maintains control of the encrypted data and doesn't need to relinquish control to the cloud provider. But key management can become an issue due to the complexity and variety of platforms in use. What's needed is client-side object encryption and integrity protection with a flexible, compatible key management solution that is both secure and easy to use.

The Solution

Zettaset's XCrypt Object is a client-side, software-only encryption solution that achieves the highest level of security for data in NetApp StorageGRID deployments. It protects against both unauthorized data manipulation as well as unauthorized data access, and it uses encryption methods that can achieve speeds of up to 10+Gbps, enabling data stores to maintain their performance. XCrypt Object also includes XCrypt Virtual Enterprise Key Manager and Virtual Hardware Security Module, highly flexible, software-based solutions that automate the management of policies that protect and control access to business-critical encryption keys. Together, these products enable data protection that scales with high-volume, cloud-based, unstructured data stores, and protect data while in transit as well as in NetApp's StorageGRID. XCrypt Object supports Amazon's S3 API and encrypts your data on the client side as it's moved from StorageGRID to S3, so it stays protected and you maintain control of your keys.

Highlights

- Designed to meet the unique data protection requirements of high-volume, cloud-based, unstructured NetApp object stores
- Software-only solution simplifies deployment, easily scales in hybrid environments, and delivers exceptional price/performance
- Highly granular, user-defined key and policy management
- Provides secure authenticated encryption to protect ciphertext from unauthorized modification
- Low cost client-side encryption solution that enables users to maintain control of their keys

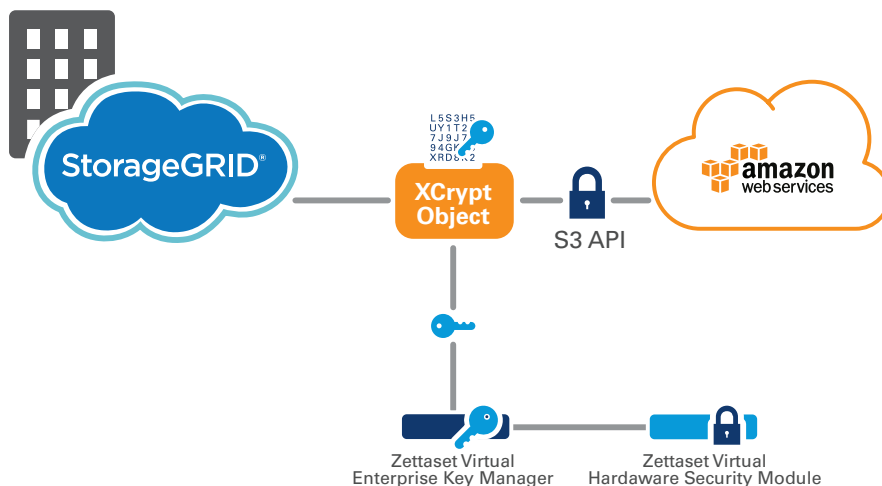
Solution Components

NetApp Products:

- StorageGRID

Zettaset Products:

- XCrypt Object
- XCrypt Virtual Enterprise Key Manager
- XCrypt Virtual Hardware Security Module



High Performance Encryption with Galois/Counter Mode (GCM)

Authenticated encryption will become mandatory due to its more stringent security properties. However, it must not compromise performance and scalability. To deliver optimal performance levels, XCrypt Object uses the Galois/Counter Mode (GCM) for authenticated encryption. GCM has been identified as the only encryption mode that addresses requirements for high data-rate authenticated encryption. GCM mode encryption can efficiently achieve speeds of up to 10+ gigabits per second and can be pipelined and parallelized.

Data Integrity Protection

There is a common misperception that encrypted data is fully protected, but even data which has been encrypted is exposed to unauthorized modification. If an attacker can write to the encrypted files (ciphertext), they can either erase data without detection, or mount a chosen ciphertext attack (CCA) to try to obtain the data key. Data-in-motion is an even easier target since an attacker can simply modify ciphertext by performing a man-in-the-middle attack. XCrypt Object addresses these vulnerabilities and includes unique features not found in any other Object data encryption solution.

XCrypt Object uses AEAD architecture to protect encrypted data from ciphertext modification, ensuring that encrypted data is verifiably secure. AEAD enables encryption and authentication to happen concurrently, making it easier to use and optimize compared to older and more commonly-used modes such as CCM. XCrypt Object can detect and mitigate the exposure associated with cyberattacks that manipulate or delete encrypted object data, ensuring the accuracy and consistency of data over its entire life-cycle.

Automated, Granular Key Management

Zettaset's key management system is infinitely scalable and highly granular, and can support unique keys per bucket, object, or group of objects. A distributed policy server enables user-defined policy enforcement on a granular level, ensuring that a "lost" key has the potential for only minor impact. Additionally, the Zettaset key manager enables administrators to set crypto policy for object encryption both on premises and in NetApp StorageGRID, promoting policy consistency. The Zettaset key manager is KMIP compatible and PKCS #11 certified, and interoperable with all major key managers and HSMs, including Thales and Gemalto.

A Software-defined Solution

Zettaset's software-only approach to encryption simplifies deployment and eliminates the need for proprietary appliances. Its configurable key policies and administration provide the flexibility necessary for your enterprise. Zettaset's products can be deployed on existing commodity hardware, drastically reducing the total cost of ownership compared to proprietary appliance-based solutions. Zettaset's products can be deployed and maintained by existing IT staff and do not require specialized encryption experts.

About Zettaset

Zettaset XCrypt is a software-defined encryption solution that can be transparently deployed across all physical and virtual enterprise environments. Unlike traditional appliance-based solutions, Zettaset is a cost-effective, software-only solution that is easy to deploy, does not impact performance, and scales from on premise to the cloud.

About NetApp

Leading organizations worldwide count on NetApp for software, systems and services to manage and store their data. Customers value our teamwork, expertise and passion for helping them succeed now and into the future.