Zettaset

DATA SHEET

XCrypt Object™

Granular, Next-Generation Client-Side Encryption with Integrity Protection for Object Data in the Cloud

Fast, Scalable, Affordable

- **Designed to meet the unique data protection requirements** of high-volume, cloud-based, unstructured object stores
- **All-software solution simplifies deployment,** easily scales in hybrid environments, and delivers exceptional price/performance
- **Highly-granular, user-defined policy management,** with support for unique keys per bucket, object, or group of objects
- **Provides ultra-secure authenticated encryption** using associated data (AEAD) to protect ciphertext from unauthorized modification
- **Protects against stealthy and highly-damaging** chosen-ciphertext attacks (CCAs)

Object storage systems continue to gain wider adoption, primarily because they enable retention of massive amounts of unstructured data. This provides companies with a simple and secure method to collect, store, and analyze large volumes of data. Object has rapidly become the storage system of choice for leading Cloud Service Providers (CSPs) like AWS and Microsoft. 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? When the CSP performs these cryptographic functions, it is called server-side encryption. When the user controls this process, it is called client-side encryption. With client-side encryption, data is encrypted on the sender's side before it is transmitted to a CSP. Client-side encryption features an encryption key that is not available to the CSP, making it difficult or impossible for a CSP to decrypt hosted data. XCrypt Object is a client-side encryption solution that achieves this highest level of protection, privacy and security for data in cloud deployments.

Why Protection for Data That's Already Encrypted?

There is a common misperception that encrypted data is fully protected, but even data which has been encrypted is exposed to malicious attacks and unauthorized modification. If an attacker can write to the encrypted files (ciphertext), they can either (1) erase data without detection or (2) 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.

Next-Generation Encryption for Added Ciphertext Integrity Protection

XCrypt Object is a true next-generation data protection solution that takes the extra step of providing integrity protection for encrypted data. XCrypt Object uses AEAD architecture (vs. Encryption + MAC) 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. This advanced capability ensures the accuracy and consistency of data over its entire life-cycle.

Authenticated encryption using associated data has additional advantages as part of the XCrypt Object encryption solution.

- **AEAD is verifiably secure**, while Encrypt + MAC is not
- **AEAD using Galois/Counter mode (GCM)** protects against an intruder writing to files at-rest by way of a chosen-ciphertext attack (CCA)
- **AEAD improves efficiencies** because of its ability to concurrently perform encryption and authentication

Some otherwise secure encryption schemes, including non- authenticated encryption modes, can allow attackers to discover the encryption keys using a CCA. Non-authenticated encryption only prevents an attacker from reading the plaintext. It does not prevent an attacker from modifying the ciphertext.

The authenticated encryption mode used by XCrypt Object is able to prove that the ciphertext was made by someone who was authorized to possess the encryption. Existing non-authenticated encryption products depend on the user to detect any data modification by noticing plaintext that appears to be wrong, an unreliable approach that exposes organizations to unnecessary risk.

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 ensure 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.

Automated, Granular Key Management

XCrypt Object's key management is 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. The automated policy server also ensures that your keys never go to clients.

Supports Strategic IT Compliance Initiatives

- **Provides a proven defense** for sensitive data in regulated industries such healthcare, financial services, and retail from the accelerating frequency and scope of data breaches
- **Supports corporate and regulatory compliance initiatives** including PCI/DSS, HIPAA, FISMA, and GDPR.

Simple to Deploy, Low TCO

- **No proprietary appliances required**, making XCrypt Object non-disruptive and much more cost-effective compared to legacy approaches. This is especially valuable in highly elastic cloud environments and provides power users with greater operational efficiencies.
- **Supports Java API and REST API** for ease of integration
- **Simplified installation using CLI tools** (Ansible, Puppet, Chef)

Fits into Existing Security Infrastructure

- **Adheres to OASIS encryption open standards**, and is compatible with KMIP-compliant key management systems and PKCS#11-compliant hardware security modules (HSMs)
- **Included with the XCrypt Hadoop data encryption solution** is a software-based automated Virtual Enterprise Key Manager (V-EKM) and Virtual Hardware Security Module (V-HSM) to facilitate initial deployment
- **AES-GCM Suite B-compliant**, works with FIPS-certified KMIP servers

Interoperability Certifications

- **Certified interoperability with key manager solutions** from MicroFocus, Fornetix, Gemalto, HyTrust, Thales and others
- **Certified interoperability with HSMs** from Utimaco, Gemalto, Thales and others

XCrypt Object is just one of the advanced, industry-leading encryption solutions built on Zettaset's XCrypt Data Encryption Platform. Additional solutions include XCrypt Full Disk and XCrypt Hadoop. For more information, please contact us at sales@zettaset.com

About Zettaset

Zettaset is a software-defined encryption solution that protects against data theft and can be transparently deployed across all physical and virtual environments. Its products are designed for medium to large enterprises that deal with sensitive information that would expose them, financially and reputationally, in the event of a breach. Unlike traditional solutions that are appliance-based, Zettaset is a cost-effective, software-only solution that is easy to deploy, does not impact performance, and scales with your business from on premise to the cloud.