z/OS data set encryption

Trust - the currency of the digital economy.

In today's interconnected business economy the use of trusted digital assets can make or break your reputation. Most organizations know that data protection and encryption play a vital role in safeguarding these critical assets. Compliance regulations also challenge organizations to encrypt their data assets and reduce risk. However, implementing an effective encryption program is fraught with implementation issues. Questions around what data to encrypt, where encryption should occur and responsibility for encryption can undermine the best data protection plan. Far too often these plans result in encryption gaps, inconsistent use of encryption and increased risk.

Encryption practices

As a practice, it is advisable to encrypt data as soon as possible ideally at the source. Today, data is encrypted at multiple points along the data journey often using different tools and different policies. This increases the administrative burden, increases complexity and adds costs without effectively protecting your data. A better approach is needed.

What is z/OS pervasive encryption?

Pervasive encryption is a transparent and consumable approach to enabling encryption of data in-flight and at-rest to simplify and reduce costs associated with protecting data and achieving compliance. z/OS® data set encryption is a key component of pervasive encryption whereby data is encrypted automatically and immediately upon data set creation. z/OS data set encryption can be performed transparently without requiring application coding changes.

To encrypt data at speed, IBM Z® can encrypt data using CPACF, on chip-based hardware acceleration. With IBM z14™ (z14), the speed of cryptographic coprocessors is designed so that high volume workloads can be easily protected while meeting target service levels.

Key management is a vital part of any encryption solution. The use of protected keys, combining the hardware protection of IBM Crypto Express adapters with the cryptographic acceleration of on chip encryption, delivers a solution with the highest protection at the best performance. Keys can also be managed through IBM's key management solutions including EKMF, Enterprise Key Management Foundation. And master keys can be securely entered through IBM's TKE (Trusted Key Entry) workstations.

In addition, IBM z/OS data set encryption is designed to be integrated with DFSMS™ and RACF® controls allowing for a central and consistent policy-based approach to encryption. You can create separate policies to govern access to files versus access to file content. The security policies can be fine or course grained to afford you flexibility to match your organization's needs. And most importantly, you can have confidence that encryption policies you define will be implemented consistently, and automatically, without gaps.

Eligible Files

z/OS offers data set encryption planned for sequential extended format data sets accessed via either BSAM or QSAM, and VSAM extended format data sets access via base VSAM or VSAM RLS. z/OS data set encryption is designed to be embedded directly in the access method in order to encrypt data immediately and automatically as data sets are created.

Support includes:

- z/OS V2.3 support; z/OS V2.2 plus service. Toleration support in z/OS V2.1
- DB2® for z/OS, V11 and V12 support z/OS data encryption at z14 GA; additional DB2 V12 support through continuous delivery
- IMS™ V14 and IMS 15 QPP program support z/OS data set encryption for select data sets CICS® VSAM files are supported
- zFS encryption of individual files and more

Labor Saving

Many clients selectively encrypt only some of their data due to the labor intensive efforts around data classification. Automatic encryption can decouple the process of implementation of encryption from the process of data classification. Data classification is typically a time consuming and error fraught process requiring coordination amongst many organizational teams. Finally encryption can be much more accessible to the organization than it has been in the past, as encryption can be easily enabled through RACF commands, SMS policy, JCL and more.

Benefits

- ✓ Protect sensitive data automatically
- ✓ Ensure that consistent policy is used
- ✓ Application transparent
- ✓ Efficient and fast on chip encryption
- ✓ Enables audit and compliance readiness
- ✓ Security benefits of protected key

Separation of Duties

z/OS data set encryption is designed to differentiate between access to files covering operational tasks like migrations and backups, and access to file content. For instance, companies may request storage administrators to access encrypted files for data reorganization, data migrations or other tasks. These individuals may not need access to privileged *content*. With z/OS data set encryption, granular access control can allow authorized staff to handle encrypted files while prohibiting access to file content. This helps enforce separation of duties and enables compliance readiness.

Remove application complexity

Today data encryption often falls on the shoulders of programmers, requiring application programming skills, maintenance of programs and coordination between different teams. One weak link in the encryption chain means that data protection can be compromised. Embedding encryption into the access method allows encryption of data in bulk at the source with no application changes required.

Audit and compliance

z/OS data set encryption is designed to allow organizations to more easily and cost effectively meet compliance and audit objectives. Customers can determine whether data is encrypted by examining their SMF data making it easy to validate whether files are meeting regulatory compliance requirements.

IBM Z at the core

IBM Z technology provides industry leading advantages with fast on chip encryption and cryptographic cards for protected key operations. z/OS data set encryption can benefit from both the security of Crypto Express adapters and the speed of on chip bulk encryption. With IBM Crypto Express adapters customer encryption keys are never in the clear, delivering security protection designed for FIPS 140-2 Level 4 certification.

Summary

Customers can encrypt critical z/OS data transparently, efficiently and automatically without the need for additional tooling or programming efforts. When used with z14, customers can leverage the increased performance of the newest Crypto Exprss6S adapter, and faster CPACF designed to deliver faster encryption and decryption than previous servers.

ZSL03418-USEN-00