IBM Z
Introduction
October 2017

Pervasive Encryption

Frequently Asked Questions

Please check for continued updates to this document

Worldwide

ZSQ03116-USEN-02

Table of Contents

Announcement 3
Requirements and support 5
Operational considerations 7
Keys and Key Management 8
Coupling Facility Encryption 9
Network Encryption and Tooling 12
Software and Services 13

Announcement

What is pervasive encryption?

At the core of every enterprise are business assets which if lost or compromised could cause irreparable damage. Core business data may be governed by regulatory requirements designed to protect data and safeguard privacy, with high penalties in the event of loss. Internal and external pressures to protect customer data have changed the perspective around how core business data should be handled.

Data becomes the new perimeter of the enterprise and must be protected. Establishing a fortified perimeter around core business data using encryption is one of the most impactful ways to help protect data and prevent loss. Pervasive encryption is enabled by administrative policy controls and is designed to be application transparent, without requiring application changes.

Pervasive encryption is a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption and reduce costs associated with protecting data and achieving compliance mandates.

The IBM Z® platform is designed to provide pervasive encryption capabilities to help you protect data efficiently in the digital enterprise.

What did the IBM z14 announcement say about pervasive encryption?

The IBM z14™ (z14) platform provides pervasive encryption capabilities designed to enable you to protect data efficiently, and without requiring application changes.

The IBM z14 platform provides the hardware infrastructure, in a balanced system design, with the encryption capabilities that now make it possible to create a fortified perimeter around critical business data. The Central Processor Assist for Cryptographic Function (CPACF), is standard on every z14 core, and is enabled via feature code #3863. The CPACF has both the cryptographic suite and performance characteristics that can enable bulk encryption of sensitive business data that makes it possible to fortify, intrinsically protecting business data using encryption technology. Working with the new Crypto Express6S feature (#0893), the key materials used to create this fortified data perimeter are protected, using the IBM Z unique protected key CPACF in which the keys used in the encryption process are not visible to the applications and operating system in clear text form.

The IBM Z operating environments, such as z/OS®, are designed to take advantage of the z14 platform imbedding the use of the z14 cryptographic engines within the operating environment to help create an environment where policies can be enforced that govern intrinsic data protection, helping clients build the perimeter around business data. For more information on IBM Z operating environments' use of the hardware capabilities of z14 see announce letter 217-246, IBM z/OS Version 2 Release 3 -- Engine for digital transformation, dated July 17, 2017.

What was announced in the July 17, 2017 IBM z/OS v2.3 announcement?

z/OS V2.3 and z14 can help drive pervasive encryption efforts within an enterprise by supporting clients in their objective to meet complex compliance mandates by creating a fortified perimeter around core business data.

z/OS is designed to provide new policy-based encryption options that take full advantage of the improvements in the z14 platform and can help clients protect their critical business data. These new capabilities include:

- Enhanced data protection for many z/OS data sets, zFS file systems, and Coupling Facility structures gives users the ability to encrypt data without needing to make changes to applications to imbed encryption APIs within applications
- New z/OS policy controls make it possible to use pervasive encryption to help protect user data and simplify the task of compliance
- z/OS Communications Server includes encryption-readiness technology to enable z/OS administrators to determine which TCP and Enterprise Extender traffic patterns to and from their z/OS systems meet approved encryption criteria and help simplify the task of compliance

What are some of the design advantages being built into z/OS data set encryption?

z/OS data set encryption:

- Uses CPACF and protected key, which means that key material is not visible in clear text format, offering a higher level of protection along with the high throughput of encryption using CPACF
- Is designed to protect data in a way that is aligned with customers' current access control mechanisms offering a more straightforward configuration experience
- Is designed to perform efficiently at speed
- Has the ability to enable encryption without requiring application or database changes
- Allows data to remain encrypted throughout its journey. For instance, with z/OS data set encryption any data replicated through PPRC or XRC, or backed up or migrated, remains encrypted
- In-memory buffer content is not encrypted which means that every data access does not require an encrypt or a decrypt operation; this design helps reduce the overall cost of encryption
- Can be configured such that encryption keys are owned and managed by logical organizational environment (e.g.; production versus test) providing cryptographic separation from other environments.
- Can help simplify clients' compliance efforts

How is data set encryption different from other encryption software that IBM offers?

Data set encryption enables encryption of files in bulk through the access method as opposed to encrypting a single field or row at a time. z/OS data set encryption is designed to offer high throughput, low cost encryption. It is intended to be more accessible to the organization than many other forms of encryption. For instance, z/OS data set encryption is designed to be transparent to the application, requiring no changes to application code. z/OS data set encryption enables customers to encrypt data at course scale without the need to perform data identification and classification first.

Is data set encryption a separately priced feature?

No, z/OS data set encryption capabilities are included as part of the base capabilities of z14 and of the operating systems; z/OS data set encryption is part of the base DFSMS™ component of z/OS V2.3. Clients are advised to order a Crypto Express Adapter priced feature in order to use protected key.

Requirements and support

What are the crypto adapter requirements for z/OS data set encryption?

Data set encryption always uses CPACF protected keys for keys in memory. Protected keys ensure the key is not visible to applications or to the operating system.

Protected keys, based on secure keys, offer the security capabilities of the Crypto Express adaptor along with the performance characteristics of on-chip crypto using CPACF. It is strongly recommended to use the Crypto Express adaptor to protect secured keys. A Crypto Express 3 or higher level adaptor is recommended for this purpose.

What Crypto Express "mode" is required to support z/OS data set encryption? Is it possible to have another mode configured concurrently on the same Crypto Express adapter?

z/OS data set encryption require the Crypto Express feature to be configured as a CCA coprocessor. A given Crypto Express feature may be configured as a CCA coprocessor, an EP11 coprocessor, or an accelerator, but can only be configured as one type at a time.

What is the minimum and recommended hardware and software for z/OS data set encryption?

Product/Feature	Required Level	Description
Hardware (HW)		
Minimum HW	z196 CPACF	Minimum HW
	Crypto Express3 or higher	Minimum HW for Secure-key/Protected-key CPACF[1]
Recommended HW	z14 CPACF	CPACF performance improvements
	z14	Enterprise Key Management Foundation (EKMF) feature
Operating System Support		
DFSMS	z/OS 2.3	Full support in 2.3, 2.2 plus service
	z/OS 2.2 + OA50569 PTFs	
	z/OS 2.1 + OA50569 PTFs	Toleration only – read/write, cannot create encrypted data sets.
RACF®	z/OS 2.3	DFP segment key label; conditional access checking
	z/OS 2.1, 2.2 + OA50512 PTFs	
ICSF	HCR77C0 or HCR77C1 when available	Protected-Key Read
	HCR77A0–B1 + OA50450 PTFs	
1– Secure-key is *strongly recommended* for production environments. Clear key can be used in dev/test.		

What does toleration/coexistence support for z/OS V2.1 mean?

z/OS V2.1 with service applied is designed to able to support z/OS data set encryption in toleration mode, meaning it can read from and write to encrypted data sets but not create new encrypted data sets.

What changes are needed to make sure that encrypted data sets created on a current IBM Z server are accessible to down-level servers with prior cryptographic capabilities?

IBM Z encryption hardware (Crypto Express and CPACF) is typically downward compatible. If prior generation IBM Z servers meet the minimum hardware and software requirements for z/OS data set encryption, they would be able to access encrypted data sets produced by z/OS data set encryption.

What files and databases can leverage z/OS data set encryption?

z/OS data set encryption supports sequential extended format data sets accessed through BSAM and QSAM, as well as VSAM extended format data sets accessed through base VSAM and VSAM/RLS.

This is aligned with clients' most immediate need to protect data associated with databases, CICS®/VSAM applications and batch workloads. Also zFS makes use of z/OS data set encryption to support the encryption of individual files (file content), access control lists, security information, and symbolic link contents.

Data set encryption is transparent to applications and data bases that call documented access method APIs for VSAM, QSAM and BSAM access methods. Applications that use the licensed Media Manager interfaces to access encrypted data sets require changes.

Are there plans for Db2 and IMS to exploit z/OS data set encryption?

Db2® for z/OS, V11 and V12 support for z/OS data encryption are available at z14 GA, September 13, 2017. Db2 12 will add support for additional DBA controls over encryption options through continuous delivery after September 13, 2017.

Db2 is designed to transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects. which could cause disruption to operations. This includes the ability to transparently encrypt its logs, catalog, directory, tables and indices including all data types such as large binary objects transparently. In addition, for maximum availability, rekeying of data keys can be performed non-disruptively without taking Db2 databases offline.

IMS™ V14 supports z/OS data set encryption for select data sets. The IMS 15 Quality Partnership Program (QPP) offering also supports these capabilities. Also, z/OS data set encryption allows customers to take advantage of transparent encryption of select IMS data sets.

Is there additional encryption support with z/VM V6.4?

With the PTF for APAR VM65993, planned to be available December 15, 2017, z/VM® V6.4 will provide support for encrypted paging, in support of the z14 pervasive encryption philosophy of encrypting data in flight and at rest. Ciphering will occur as data moves between active memory and a paging volume owned by z/VM. Included in the support is the ability to dynamically control whether a running z/VM system is encrypting this data.

Would customers be able to use both encryption *and* compression?

Yes. Since encrypted data does not compress, data must be compressed first before it is encrypted. For encrypted, compressed data sets the access methods perform both compression and encryption operations and will compress data before the data is encrypted, and decrypt data before it is decompressed.

Operational considerations

How should my customer modify their cryptographic environment to prepare for z/OS data set encryption?

Customers can install Crypto Adapters on supported servers and can also plan to configure their environment to support protected key environments. Customers need to install and configure ICSF. ICSF callable services and programs help users generate, maintain, and manage keys. ICSF provides APIs by which applications request cryptographic services. Customers must also configure a CKDS data set to store keys. Data set encryption requires the use of AES master keys.

Is there CPU overhead when using z/OS data set encryption?

Encryption typically consumes processor cycles. z/OS data set encryption is designed for performance and efficiency offering design elements to reduce cost. For instance, z/OS data set encryption is performed at the I/O buffer write level in order to keep encryption more cost effective than encrypting a single record at a time. The use of the Crypto Express adapter is optimized and is used initially at data set open time to handle processing of the key after which CPACF is used for high performance and efficient data set encryption. ICSF is also optimized to cache keys so that when a data set is re-opened, the protected key is accessible, avoiding additional I/O costs. An enhanced zBNA tool is planned to help users and IBMers estimate the CPU cost of encryption as part of their planning efforts.

Is it possible to backup and restore encrypted data sets "as-is," without decryption?

Yes, DFSMSdss™ and DFSMShsm™ provide a number of utilities and copy functions such as copy, dump, restore, PPRC and more that support encrypted data sets without the need to access data in the clear. Data sets remain encrypted throughout this processing. The ability to perform these utility functions without requiring key label access to decrypt data is an advantage and can help with compliance efforts.

Are there any planned tools to assist clients with estimating the CPU cost of encryption?

Yes. The zBNA tool has been enhanced to help estimate additional CPU incurred when enabling encryption for certain workloads. It can also be used to help estimate CPU costs for both data set encryption and also for coupling facility encryption. Customers will need to use the zBNA V1.8.0 tool with DFSMS, RMF™ and XES PTFs applied when available.

How can I avoid delays in z/OS initialization and termination when using data set encryption?

Customers need to ensure that ICSF is started early in the IPL process to avoid delays in z/OS initialization and termination. This is especially true if customers plan to encrypt SMF data sets or other data sets used during z/OS initialization. As such, it is highly recommended the command S CSF,SUB=MSTR (or appropriate PROC name) is placed early in the COMMNDxx member to ensure there is minimum delay in z/OS initialization. Specifying SUB=MSTR is necessary to allow ICSF to start before JES. Furthermore, during z/OS system shutdown, ICSF should be one of the last features to be terminated so that dependent functions are not impacted. It is highly recommended that ICSF be brought down after terminating the JES address space and after initiating SMF halt processing. Note that since ICSF is brought down after SMF is halted, there may not be an SMF record cut for the termination of ICSF.

Keys and Key Management

Does z/OS data set encryption allow for the use of different keys to protect different data sets?

Yes, customers can assign different keys using different RACF profiles and DFSMS classes. Customers do not need to define a unique key for each and every data set encrypted, and groups of data sets can share common keys. This can help simplify administration.

How do customers create keys and key labels?

Clients will be able to define, generate and store a key in ICSF. ICSF web deliverable HCR77C1 offers enhancements to help simplify key management. The CKDS browser is designed to make it easier for ICSF administrators to manage the life cycle of their cryptographic key material that resides in the CKDS. The CKDS browser can help customers new to ICSF provision encryption keys for applications and for use by z/OS.

Clients can also use EKMF to generate and manage keys. Once the key label is defined, the key label would be associated with a particular data set or group of data sets through several methods offering flexibility and choice. Clients can also use ICSF services to help manage keys.

What type of encryption does z/OS data set encryption use?

z/OS data set encryption is designed to use AES 256, considered one of the strongest.

Is it possible to expire, revoke, and/or reissue keys related to z/OS data set encryption?

Newer versions of ICSF support key record metadata for expiring and archiving encryption keys. Enterprise key management systems can also provide this capability. It will be possible to rekey data by generating a new key and key label, assigning a new key label to a new data set and migrating data encrypted under old key to the new key by copying the data set to the newly created data set.

Coupling Facility Encryption

What is Coupling Facility encryption?

Regarding Coupling Facility (CF) encryption z/OS V2.3 provides support for end-to-end encryption for both coupling facility data in flight. and data at rest in coupling facility structures.

The CF image itself never decrypts, nor encrypts, any data. Host-based CPACF encryption is used for high performance and low latency encryption.

z/OS V2.3 uses CPACF encryption to encrypt and decrypt CF data as it is sent to and returned from the CF. The data is encrypted as it travels on the CF link and remains encrypted while resident in the CF.

CF Encryption is supported only by z/OS V2.3 and is not supported by z/OS 2.2 nor by any other down level z/OS release.

Is coupling facility encryption a separately priced feature?

No, Coupling facility encryption is available with z/OS V2.3, and is not a separately priced capability.

What are some of the design advantages of CF encryption?

CF Encryption is designed to perform at speed and with minimal CPU overhead. There are no application changes required to use CF encryption. CF encryption allows data to remain encrypted throughout its journey across the sysplex including while data is at rest in the coupling facility itself. CF encryption:

- Uses CPACF protected key, which means that key material is not visible in the clear
- Is designed to perform at speed with minimal overhead
- Encryption is enabled without needing to make application or database changes.
- Encrypts data across the sysplex, helping customers meet compliance requirements

What coupling facility control code requirements are required to use coupling facility encryption?

IBM z14 CFLEVEL 22 CF images are not required, but are recommended in order to simplify sysplex recovery. A (relatively rare) sysplex wide-outage recovery scenario in which the sysplex is re-IPLed using newly-formatted CFRM couple data sets, would benefit if the encrypted structures were residing in a CFLEVEL 22 CF.

Also, IBM z14 z/OS images are recommended for improved AES CBC 256 encrypt/decrypt performance on z14.

Is there CPU overhead for CF Encryption?

Coupling Facility encryption is host based and does not occur on the coupling facility. All host encryption consumes processor cycles, but IBM CPACF encryption is very designed to be efficient. Encryption on IBM z14 is fast; *CPACF encryption rates for like modes and data sizes on z14 are up to six times faster than on the* IBM *z13®*[1].

Note 1. Disclaimer: Based on preliminary internal IBM lab measurements on a standalone dedicated system in a controlled environment and compared to the z13. Results may vary.

How does one encrypt Coupling Facility structures?

Users can select precisely which structures to encrypt and coupling facility structures are defined with their own unique keys. Encryption of each CF structure is controlled through a new z/OS Coupling Facility Resource Management (CFRM) policy keywords:

ENCRYPT(NO): means the structure should NOT be encrypted (the default)
ENCRYPT(YES): means the structure should be encrypted

Note that data flowing between z/OS and the CF is encrypted as the intent is to encrypt all data that might be sensitive. Internal control information and related metadata is *not* encrypted

What data is eligible for Coupling Facility encryption?

z/OS V2.3 gives users the ability to encrypt Coupling Facility data, including list and cache structures, under the control of the Coupling Facility Resource Management (CFRM) policy. Lock structures are not encrypted as they do not contain any user data.

What are the minimum requirements for coupling facility encryption?

The minimum IBM Z server required is the IBM zEnterprise® EC12 (zEC12) but z14 z/OS images are recommended in order to obtain AES-CBC 256 CPACF encrypt/decrypt performance improvements. In addition a Crypto Express3 adapter or higher is required.
From an operating system support, note that z/OS V2.3 is the base level required for CF encryption.
A pre-z/OS V2.3 system cannot connect to an encrypted structure. If a pre-z/OS V2.3 system is connected to a structure, the structure cannot be encrypted. Toleration support must be applied to down level z/OS systems.

Please see table below for required support.

Product/Feature	Required Level	Description
Hardware		
z/OS: Minimum HW	zEC12	Minimum supported for z/OS 2.3
	Crypto Express3	Required for Protected-key CPACF
z/OS: Recommended HW	z14	AES-CBC CPACF encrypt/decrypt performance improvements
CF: Recommended HW	z14	Simplified recovery for specific sysplex-wide reconciliation scenarios
Operating System – Base Support		
z/OS	z/OS 2.3	z/OS support for CF encryption
Additional Support		
zSecure®	zSecure 2.3	zSecure Audit support for CF encryption
zBNA	zBNA	zBatch Network Analyzer support for CF encryption

Is there CF encryption toleration support for z/OS V2.1 and 2.2?

CF encryption is available with z/OS v2.3, and is not available for down level systems. Toleration APAR OA52060 for z/OS V2.1 and z/OS V2.2 prevent customers from using encrypted CF structures, allowing for z/OS V2.2 and 2.1 coexistence with encrypted structures in a sysplex.

What is the impact of master key changes?

z/OS generates the required encryption changes and handles master key management tasks. All systems in the sysplex are notified of the master key change. The structure keys in the active CFRM CDS are re-wrapped with a new master key. A change to the master key does not require data in an encrypted structure to be re-encrypted via a structure rebuild. The change affects the "wrapper" for the key, not the key itself, nor the encrypted data within the coupling facility structure.

Network Encryption and Tooling

How can the approach of pervasive encryption apply to data in flight?

z/OS already supports multiple industry standard network security protocols:

- Transport Layer Security (TLS) versions 1.0, 1.1 and 1.2
- Secure Sockets Layer (SSL), versions 2 and 3 (although the use of SSL is not recommended)
- IPsec, including Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) versions 1 and 2
- Secure Shell (SSH) version 2

The z/OS implementations of these protocols support modern cryptographic algorithms like AES-128 and -256 (each in multiple modes), SHA-256, -384 and -512, as well as RSA and Elliptic Curve asymmetric algorithms. All implementations also make full use of IBM Z hardware cryptographic support. Additionally, z/OS Communications Server provides Application Transparent TLS (AT-TLS) which allows you to apply TLS/SSL protection to your TCP-based application traffic without having to modify any application source code in most cases.

Are there tools to help understand what records are already encrypted over the network?

To address the goal of reducing costs associated with achieving compliance mandates, z/OS V2.3 Communications Server includes z/OS Encryption Readiness Technology (zERT) to help administrators determine which TCP and Enterprise Extender (EE) traffic patterns, both to and from z/OS systems, meet client encryption criteria. With zERT, SMF records can be collected to build a record of the cryptographic protection of each TCP and EE connection.

zERT summary record support is planned as a post-GA deliverable in first quarter 2018 with the PTF for APAR PI83362

Software and Services

Will IBM security software such as IBM Security zSecure support pervasive encryption?

Yes, IBM Security zSecure suite V2.3 helps administer and audit pervasive encryption capabilities. zSecure allows clients to immediately audit and monitor usage of data set encryption features. zSecure can help customers understand which systems and which users can decrypt data, aiding in the administration and control of pervasive encryption. zSecure also helps with direct navigation from data set encryption key labels to the administration of key label protection profiles. In addition, key labels can be enriched with selectable key algorithms and key length fields. The report type SMF adds 118 new fields for the new zERT Encryption Readiness Technology SMF record 119-11. zSecure also collects, formats and enriches pervasive encryption information that is sent to SIEMs including IBM QRadar® for enhanced enterprise-wide security intelligence.

Are there IBM resources available to help clients assess their readiness for pervasive encryption and to assist in addressing any gaps?

Yes, IBM Systems Lab Services has a Pervasive Encryption Readiness Assessment, and a full set of offerings to execute the various levels of encryption and security. You can contact IBM Systems Lab Services via the Internet at: https://www.ibm.com/it-infrastructure/services/lab-services or send an email to ibmsls@us.ibm.com

For clients interested in fully utilizing security capabilities of the z14, but currently using non-IBM security software, are there resources available to help with migration to IBM products?

Yes, IBM Systems Lab Services can help you with migration from non-IBM security software, and can help implement IBM hardware and software security capabilities. You can contact IBM Systems Lab Services via the Internet at: https://www.ibm.com/it-infrastructure/services/lab-services or send an email to ibmsls@us.ibm.com

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
Produced in the United States of America,
10/2017

ZSQ03116-USEN-02