PKWARE®

Mainframe Cryptography:
Discovering a Better Way

TECHNICAL WHITE PAPER

Table of Contents

Mainframe Cryptography: Discovering a Better Way

Sensitive enterprise data is at risk to outside breaches and from malicious attacks of employees inside the organization. Moving quickly to implement a data security solution can contribute directly to risk reduction and potential costs associated with "after the fact" remediation. Many organizations want to believe their defenses can never be breached, that errors of inattention or neglect will not occur, and no insider will ever misuse sensitive data. Yet, again and again, large organizations with well trained technical staff lose control of sensitive data resulting in great cost - recent surveys indicate that a data security breach in the United States is remediated at a cost of over $200 per customer impacted, with an average total cost above six million dollars.

In response, persistent data protection for both data-at-rest and data-in-motion is now the assumed minimum standard-of-care for the enterprise. As Forrester frequently has commented over the last several years, and as recently as October of 2009[1], the need for strong data security has gone beyond perimeter-centric data protection alone. It now requires supplemental protections that remain with all types of data, wherever it is and wherever it goes. Strong encryption is an accepted practice for achieving such persistent, portable protection.

Organizations recognize this need while at the same time struggling with the implicit introduction of additional costs to their operations. For some, the combination of the operational overhead of encryption, the inherent need for secure encryption key generation & management, and the burden of appropriate data security policy enforcement functions introduces unsupportable new complexity and cost. Fortunately, there are ways such costs can be contained, and in some cases, even reduced to have negligible

[1] See "Data Security: One of Forrester's Top 15 IT Technologies to Watch," http://blogs.csoonline.com/data_security_one_of_forresters_top_15_it_technologies_to_watch

impacts on operational budget. IBM®'s z/OS® and the mainframe hardware supporting it form the foundation for efficient strong data encryption, safe key generation and management, and sound data protection policy enforcement. Combined, these capabilities offer a cost-effective option for safeguarding organizations' digital assets; however, taking advantage of them presents some challenges.

Reducing the Overhead of Strong Cryptography

Encryption, by its nature, is computationally intensive. The work required to sufficiently randomize data in a manner that allows it to be later restored to a readable state far exceeds the effort required to simply write the data from one location to another. This has frequently been the obstacle that prevents many organizations from including this useful operation in their data workflows. The mainframe offers some unique advantages fitted to this need with hardware cryptographic acceleration.

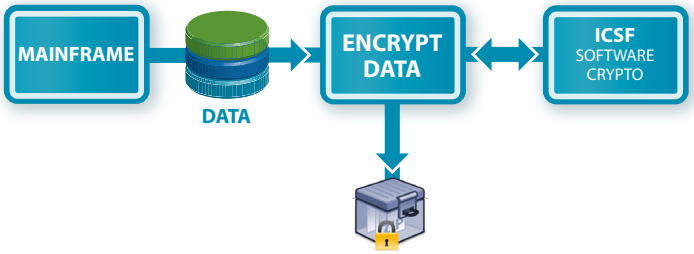

FIGURE 1: ENCRYPTION USING ICSF SOFTWARE CRYPTO

Unlike many other contemporary computing platforms, IBM z9® and z10® mainframes include hardware-based cryptographic acceleration natively and, in fact, offer multiple options to reduce the capacity required to encipher data. Hardware-based cryptography (encryption/decryption, hashing, and PRNG performed using direct calls to the hardware's instruction set) always requires fewer resources than cryptography performed using software alone. The overhead of system management, command interpretation, and other operations required when processing software applications is avoided. Contemporary IBM mainframes offer at least two approaches for reducing the cryptographic calculation load for a given operation:

- CPACF - Central Processor Assist for Cryptographic Function
- CEX2C - Crypto Express 2 Coprocessor

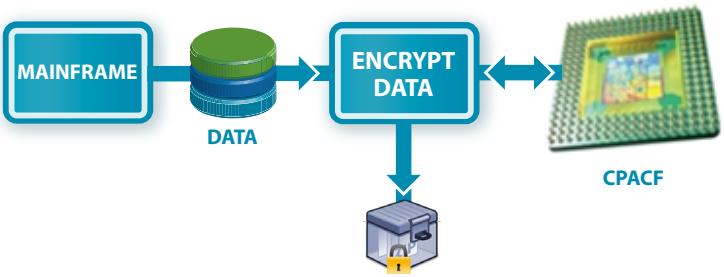

FIGURE 2: ENCRYPTION USING CPACF HARDWARE CRYPTO

In all cases, the hardware processes the largest majority of the cryptographic calculations, reducing by an order of magnitude the burden on the general purpose CP compared to the same operation performed in software.

For example, assume a 2096-O04 mainframe that encrypts a one gigabyte transaction log for secure storage five times each hour. Using the IBM software encryption available through the Integrated Cryptographic Services Facility (ICSF), 126.14 CPU seconds are required. Using the same machine and the IBM CPACF hardware encryption acceleration available directly from the CP instruction set, the same job requires only 18.62 CPU seconds, a difference of 107.52 CPU seconds per run[2] . Assuming this process continues throughout a given year, use of the hardware encryption facility could reduce the amount of capacity that is required for a given machine or LPAR:

CPU Second-to-MSU Instance Calculation	
Mainframe Model	2096-O04
SU/Sec Rating from Watson Report	6,015
Number of CPs	4
Total Available SU/Sec	24,060
Seconds/Minute	60
Minutes/Hour	60
Available SUs per hour	86,616,000 1,000,000
Convert to H/W MSU	87
S/W MSU from Watson Report	67
Conversion Factor	0.77

(the basis for the MSU rating of the machine)

Instance Formula	
CPU Second savings/job	107.52
Times jobs run per hour	5
Total CPU Seconds used	538
Total # of CPU Seconds/hour	14,400
SU/Sec	24,060
Total SUs used for instance	12,934,656
SU/Sec to H/W MSU conversion factor	1,000,000
Instance H/W MSUs used	12.93
Model H/W MSUs to S/W MSUs conversion factor	0.77
Instance S/W MSUs used	10.01

(4 CPUs x 60 seconds x 60 minutes)

FIGURE 3: CPU SECOND SAVINGS CONVERTED TO MSUs[3]

This could mean the difference between remaining with a 2096-O04 and forestalling an upgrade to a P04 or larger machine. While the capacity savings would be specific to each organization, the complete complement of software installed, the agreements with IBM and the ISVs providing such software, the total cost postponed, or avoided altogether, could be substantial.

However, manually integrating this facility into existing and new workflows is time-consuming and expensive, particularly for organizations unfamiliar with the intricacies of IBM encryption; organizations need a better way.

[2]Please contact your PKWARE representatives for a complete profile of the mainframe used for this benchmark, and of the benchmark procedure.

[3]For more information on this calculation, please see the PKWARE paper "Rationalizing CPU Second Reductions to MSU Capacity" due November 2009.

Protecting & Managing Cryptographic Keys

Encryption efficiency is, of course, immaterial without the availability of durable encryption keys and the diligent protection of decryption keys[4]. Devising the appropriate scheme to protect such keys and to ensure that key use is controlled in an auditable manner has defeated many early implementations. Both the cost of developing the necessary scheme ad hoc and the cost of purchasing packaged software products for this purpose have been seen as burdens too great to bear. Moreover, most (if not all) packaged solutions either failed to cover all types of keys or sat outside the rigorous protections available on the mainframe.

Practically speaking, both an encryption and a decryption key are required for every encryption use, and such paired keys come in two different types: symmetric and asymmetric. With symmetric keys, the key used for encryption and decryption remains the same. More colloquially, this is a password, a shared secret between the encrypting person or organization and the decrypting entity. This presents an obvious risk from insider compromise – if an encrypting operator knows the password or passphrase, it can be used maliciously. The operator can sell it to a third party who could intercept the encrypted material or make a copy of the encrypted data and decrypt it for fraudulent use later and elsewhere, etc. Maintaining a separation of duties between a security professional who manages such passphrases and the operators who execute jobs that require them is a significant challenge, multiplied when the additional requirements of appropriate logging for audit and compliance review are added. Building such functionality is onerous, particularly because this area of information technology is outside of all but a few organizations' core competencies. Building that competency in-house or contracting for it can be very expensive.

Separating passphrase management from job execution is possible with the IBM mainframe. Machines that include the PCIXCC or CEX2C or z9/10 machines with ICSF version HCR7751 applied offer the capability to segregate key management from key use via the Cryptographic Key Data Set (CKDS). However, the facilities that support this capability generally lie outside the areas most engineers have worked with. Learning to use the interfaces correctly and in a manner that satisfies internal and external auditors can be very time consuming and prone to error. The industry seeks a more cost effective approach.

The second type of encryption/decryption keys, asymmetric keys, addresses some of those issues. This area of information technology, called public key cryptography[5], relies on a branch of mathematics focused on factoring prime numbers, and can relate two keys in a manner whereby knowledge of one key in no way provides any means for deriving or reverse engineering the companion key of the pair. This greatly mitigates the risks of key management – an operator can have knowledge of and access to a public key used to encrypt sensitive data for a recipient but has no access to the private key needed for decryption; therefore, the operator has nothing of value to use or sell to a malicious third party.

However, the applications that implement the complex prime number mathematics, called certificate authorities, have been expensive to license and/or difficult to secure since they were implemented for open system architectures. The latter is a crucial issue – if a certificate authority on a Windows or UNIX platform is compromised, a data thief could have access to all the key pairs it has generated. Again, concerned professionals seek a more cost effective approach that also offers the appropriate level of security. IBM recognized these needs and provides the foundation to meet many of them. In recent z/OS promotion, IBM has positioned the mainframe as the best and most secure platform for secure key management[6]. A certificate authority is included in the operating system at no additional cost and brings the benefit of "gold standard" protection and logging for audit of the mainframe security servers. The key generation capabilities with their associated centralized key stores can be used by a variety of mainframe applications, greatly reducing the overhead of administering proprietary key stores.

[4]See http://en.wikipedia.org/wiki/Key_(cryptography) for a general discussion of cryptographic keys

[5]See http://en.wikipedia.org/wiki/Public_key_cryptography for a general discussion of public key cryptography

[6]http://www.ibmsystemsmag.com/mainframe/marchapril08/features/19601p1.aspx#

Still, the finer points of integrating with these IBM facilities are unfamiliar to most and present a daunting challenge even for seasoned mainframe engineers unfamiliar with the domain. Poorly implementing key management could be more expensive and introduce more risk than forgoing key management altogether. The market needs a better approach.

Enforcing Data Protection Policy

Encryption is a powerful tool and, like all powerful tools, it can cause great damage if not used correctly. Used appropriately, it addresses specific needs, mitigating risks to the confidentiality of sensitive information. Used inappropriately, data could be encrypted with a passphrase and held for ransom, something that has been documented as an occurrence by outside attackers[7] ; and it could even more easily occur by a disgruntled insider with access to encryption software licensed by the employer. Encryption must be subject to appropriate control and supervision to be useful to the organization.

Moreover, control alone is not enough. Not only must the organization ensure that appropriate oversight is imposed, it must also guarantee that such oversight includes appropriate logging of actions so that they can be audited at a later time. Each change to security policy must be documented, including the time, date, operation applied, and who initiated the change. If a compliance officer or an auditor requests proof that the appropriate controls are in place and are indeed having the desired effect, it is imperative that the organization have the appropriate records readily at hand to ensure that data security policies are in place and that they cannot be changed or circumvented.

While the Security Servers available to z/OS provide the infrastructure for satisfying these needs, imposing the control on the native IBM encryption facilities - or to packaged applications that are not specifically integrated with them - poses an onerous, expensive and complex effort. A better way is needed.

A Better Way…

PKWARE has provided applications tailored for the mainframe data center for over 15 years, natively implementing first for MVS, then OS/390, and now for z/OS. The version 11 release of the product focuses on meeting the market needs recounted above. It provides a cost-effective, easily integrated packaged solution that allows organizations to integrate encryption and key management facilities into existing and new workflows, and offers fully productized and supported integration with the IBM facilities for encryption acceleration, key generation and management, and encryption policy configuration, enforcement, and oversight[8] :

- Reduced administrative burden by using the common key repository used by other applications, SecureZIP for z/OS v11 can reduce key management effort, thereby reducing administration and expense
- Increased separation of duties for passphrase management, providing segregation of roles between the security administrator and the systems engineer reduces risk
- Superior data protection policy control and policy change audit

SecureZIP for z/OS v11 allows organization to standardize on a single set application that naturally integrates into existing and new workflows. Using this packaged product, organizations can quickly protect sensitive data that may be stored locally, on media, or exchanged across operating system boundaries, across geographically dispersed locations, or with customers, vendors, and partners[9] .

---

[7]'Virginia Patient Records Held for Ransom', 6 May, 2009: http://news.softpedia.com/news/Virginia-Patient-Records-Hold-for-Ransom-110873. shtml

[8]For a technical discussion of the functionality, please see PKWARE Application Note "SecureZIP Integration with z/OS Security Server Facili ties", April 2009.

[9]For a discussion of SecureZIP's cross operating system portability, please see the "SecureZIP Family Brochure" available from your PKWARE representative, or http://www.pkware.com/software-data-security/intro. For a discussion of SecureZIP PartnerLink, which grants customers license to use SecureZIP for z/OS)or for other server platforms) and the right to distribute an unlimited number of SecureZIP Partner licenses to an unlimited number of partners for any and all supported platforms, please see the "SecureZIP PartnerLink" datasheet available from your PKWARE representative, or http://www.pkware.com/software-data-security/software-secure-information-exchange.

Conclusion

Best practices and expected standards of care for data protection continue to evolve, as both the risks are more clearly identified and the monetary impacts of data breaches are more accurately estimated. All organizations seek a better way – a better way to protect sensitive data with strong encryption while still remaining operationally efficient, a better way to protect and manage the keys necessary to ensure that the encryption applied is sufficiently durable to resist attack, and a better way to impose appropriate data encryption policy reliably. For your mainframe data, SecureZIP for z/OS is that better way.

About PKWARE

PKWARE, Inc., the largest global software company providing ZIP solutions, is the creator and continuing innovator of the ZIP standard. PKWARE products are used to ensure the security and portability of data internally, as well as with partners, across all major platforms. Hundreds of global organizations in financial services, banking, retail, healthcare, government, and manufacturing use PKWARE services daily. PKWARE products provide unmatched scalability, ease of use and deployment, making them the most cost-effective means of securing data and complying with industry regulations. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York, the United Kingdom and Japan.

United States
648 N. Plankinton Ave., Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

UK/EMEA
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom

PKWARE®