Tutorial: Crypto on z/OS Systems for CIOs and the Rest of US

Greg Boyd (gregboyd@mainframecrypto.com)

Stu Henderson (stu@stuhenderson.com)

Abstract

This session is for CIOs, security administrators, system programmers, and auditors who have heard about Cryptography (both hardware and the ICSF software with z/OS), know it's important, but don't really understand it.

You may have felt that other cryptography presentations went over your head.

In this session, Greg and Stu tell you just what you need to know, in simple, understandable terms. You'll learn to cut expenses while improving security.

Agenda

1. **Introduction**
2. **The Easy, No-Brainer Steps**
3. **The Necessary Hard Part**
4. **Summary and Call to Action**

Cryptography is

The practice … of techniques for secure communication in the presence of third parties.

(from Wikipedia https://en.wikipedia.org/wiki/Cryptography)

It relies on mathematical algorithms and a unique number, called a key.

The recipient can reverse the process to recover the original data (as long as the key is secure).

Cryptography can provide

- Protection of data
- Data integrity
- Authentication (prove someone's identity)
- Non-repudiation (prove who a message came from, and that it hasn't been altered)

A long time ago

Each application tried to write its own encryption routines, often without mathematical rigor.

Results were often: inconsistent, vulnerable, costly, inefficient, difficult to administer, difficult to maintain.

Then new regulations and new technology came along, making it harder to keep up.

So IBM offered us IBM's Crypto Infrastructure on z/OS Systems (Crypto hardware plus the ICSF software). This offers a single, integrated way to do cryptography, rigorous and efficient security and integrity for our data.

What You Need to Know

Cryptography can be done in hardware or software

Any program (product, component or application) can leverage the crypto infrastructure to secure your data.

Each shop needs to enable the infrastructure and implement the products, components or applications to leverage that infrastructure.

Cryptography

Is going to be required in more and more applications

The cost can be significant, if not managed

The administrative overhead can be significant, if not managed

You need both crypto hardware and ICSF software to provide effective security and integrity on z/OS with minimum cost and minimum overhead

Two big types of change

make it important to centralize administration for encryption:

Technology (new algorithms, policy based encryption, new hardware, new password crypto)

Regulatory change (What's happening in Europe, in US)

Plus centralized key management and consistency

Three Key Risks:

If you lose the keys, you've lost the data forever.

Anyone who can see the keys and access the encrypted data can decrypt the data.

Applications can start encryption without documentation, backup, CPU tuning

Effect: No one wants this responsibility

The Main Risk:

Without formal, centralized control over keys, you risk: loss of essential knowledge and data, duplication of effort, unnecessary costs.

You'll miss technology and regulatory changes.

You can't expect some sysprog to manage this alone. The CIO needs to dedicate the resources and enforcement to have key management done simply and reliably.

Some Driving Factors

- New York State, EU GDPR (General Data Protection Regulations), PCI, CMS, NIST, and Others implementing new regulations and standards

- Policy based encryption (for data sets)

Instructive Stories From Other Shops

- The shop with hardware disk encryption
- The shop where CPU usage escalated suddenly
- The shop where they lost the master key
- The shop where the keys were exposed
- The shop where the DBA told DB2 to start encrypting
- The shop that paid too much for software licensing
- The shop that couldn't tell the auditors what was being encrypted

The Essential Take-Away

You need formal key management, no matter what the platform, with adequate: enforcement, resources, written procedures, and involvement from several key disciplines.

This doesn't work unless it comes from the CIO

Three Components

Hardware: Two devices

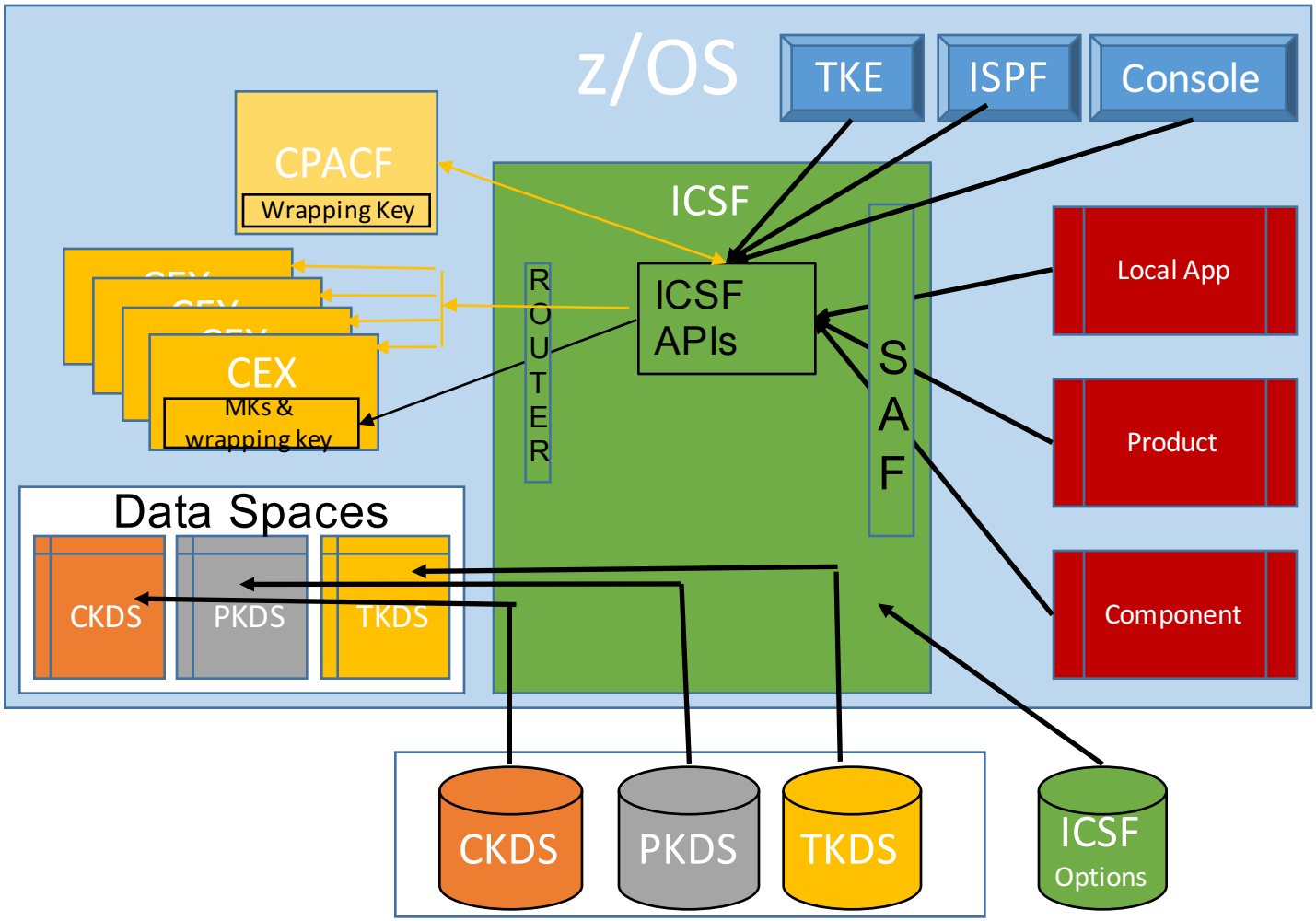
- CPACF (**CP Assist for Cryptographic Function)** - already there on your system, adds instructions to CPU, speeds processing by factor of 1000 or more
- CEXn (**Crypto Express**) - separate devices, separate price; tamper resistant; uses less CPU time, more wall clock time

  (Think "Mission Impossible")

Software

- ICSF or **Integrated Cryptologic Services Facility** (started task routes crypto requests; central control point)

ICSF Started Task

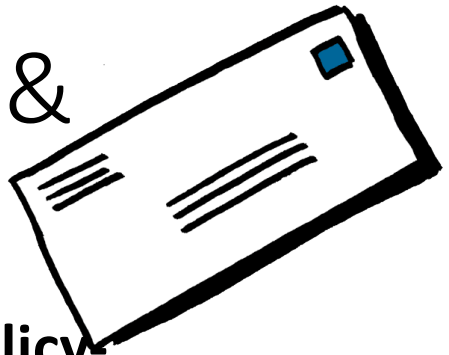


ICSF is required:

- To use the Crypto Express cards (security for key material, performance for TLS/SSL operations)
- To perform key management, including security and integrity of key material
- To support future policy based encryption of data at rest
- Many other products, such as the Infosphere Guardium Data Encryption Tool for DB2 and IMS or the Encryption Facility for z/OS

SSL/AT-TLS Exploiters

IBM Announcements 216-391 & 217-085



- IBM plans to deliver **application transparent, policy-controlled dataset encryption** in IBM z/OS. IBM DB2 for z/OS and IBM Information Management System (IMS) intend to exploit z/OS dataset encryption.
- z/OS V2.3 plans to **replace application development efforts with transparent, policy-based data set encryption**:
  - Planning enhanced data protection for z/OS data sets, zFS file systems, and Coupling Facility structures to give users the ability to encrypt data without needing to make costly application program changes.
  - Designing new z/OS policy controls to make it possible to use pervasive encryption to **protect user data and simplify the task of compliance**.
  - z/OS Communications Server will be designed to include 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 which do not.

Pervasive Encryption

- Multiple File Types
  - BSAM/QSAM
  - VSAM Extended Format
- Coupling Facility
- Encrypted data sets
  - Key labels supplied at allocation
    - RACF data set profile, DFP segment
    - JCL, Dynamic Allocation, TSO
    - SMS Data Class
    - IDCAMS

Pervasive Encryption - PreReqs

- z196/z114 or higher with CEX card
- z/OS 2.2, z/OS 2.3
  - z/OS 2.1 with maintenance can read/write encrypted data sets, but can't create an encrypted data set
- ICSF HCR77C0 or HCR77A0-HCR77B1 with OA50450
  - SYMCPACFRET(YES)
- Extended Format data sets

The Easy, No-Brainer Steps

You already have the first hardware device for free:

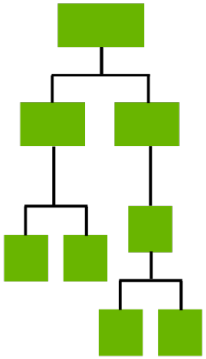
- CPACF (**CP Assist for Cryptographic Function)**

You already have the software for free:

- ICSF or **Integrated Cryptologic Services Facility**

The Crypto Express card is a tougher decision, but you're probably going to need it sooner or later

Organizational Issues



- Many parts of the organization need to be involved in defining the crypto environment:
  - Legal, regulatory, compliance, audit, risk management
  - Application owners and designers
  - Marketing
- When the demand comes from regulators, auditors, the marketplace, you need to be ready

What CIOs Need to Know and Do:

- Take ownership of encryption across the Enterprise
- Identify & Prioritize the crypto resources that require protection (Network communications? Databases? Files being sent to a partner?) What compliance regs or audits are you trying to pass?
- Define the security strengths required (AES vs TDES; RSA, ECC or both? Key lengths, Key Rotation policy)
- Identify key managers
- Inventory/purchase the tools available to meet those requirements

What Sysprogs Need to Know and Do

- Configure hardware for redundancy and recoverability
- Set up started task (Coordinate with security administrator)
- Set up key datasets
- Install and implement the tools to protect the corporate resources that need to be protected

What Security Admins Need to Know and Do

- Define userid for started task
  - Keystore access
  - USS security implications for TCP/IP
- Develop key labeling conventions (used to secure the key)
- Define Crypto Resource Rules
  - Protect the functions
  - Protect the keys
  - Define keystore policies
- Identify owner (who approves the rules)
- Document approvals, Annual re-certification, Maintain the rules

What Key Admins Need to Know and Do

- Master Keys
  - Understand the process for loading and changing master key material
  - Ensure the security of master key material that must be available for recovery purposes
- Operational Keys
  - Use Key Generation Utility Program to define symmetric keys
  - Use RACDCERT (or equivalent) to define public/private key material

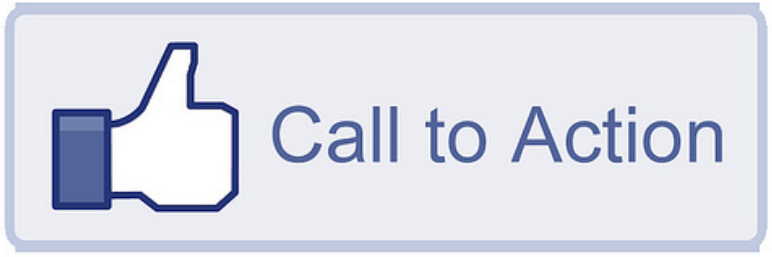
Execute key change policies

What Auditors Are Going to Expect

- Review risk assessment: who decides (who is responsible for) deciding when and how to encrypt
- Review procedures to make it happen
- Review assignment of responsibility, policy, baselines,
- Compare security software rules to approvals
- Conclude how well risk is managed

Summary and Call to Action

- The need for mainframe cryptography is unavoidable.
- If it is not managed from the CIO down, the odds of failure go up.
- You can start with the easy steps, and then dedicate resources to the hard ones.



Summary and Call to Action

We've talked about the crypto infrastructure, and why it's important, both to save money and to provide effective security.

No one person can get it properly implemented; several key players have important roles.

If these functions aren't happening in your shop, who needs to be involved to make it better?

If not you, then who?

Thanks for your kind attention

Other Info Sources

- Greg's newsletter, articles…
  - http://www.mainframecrypto.com/articles/
- Stu's newsletters, articles
  - http://www.stuhenderson.com/Newsletters-Archive.html
- IBM Crypto Education
  - https://www.ibm.com/developerworks/community/groups/community/crypto


Questions