z/TPF V1.1

TPF Users Group Spring 2008

z/TPF Cryptography Update

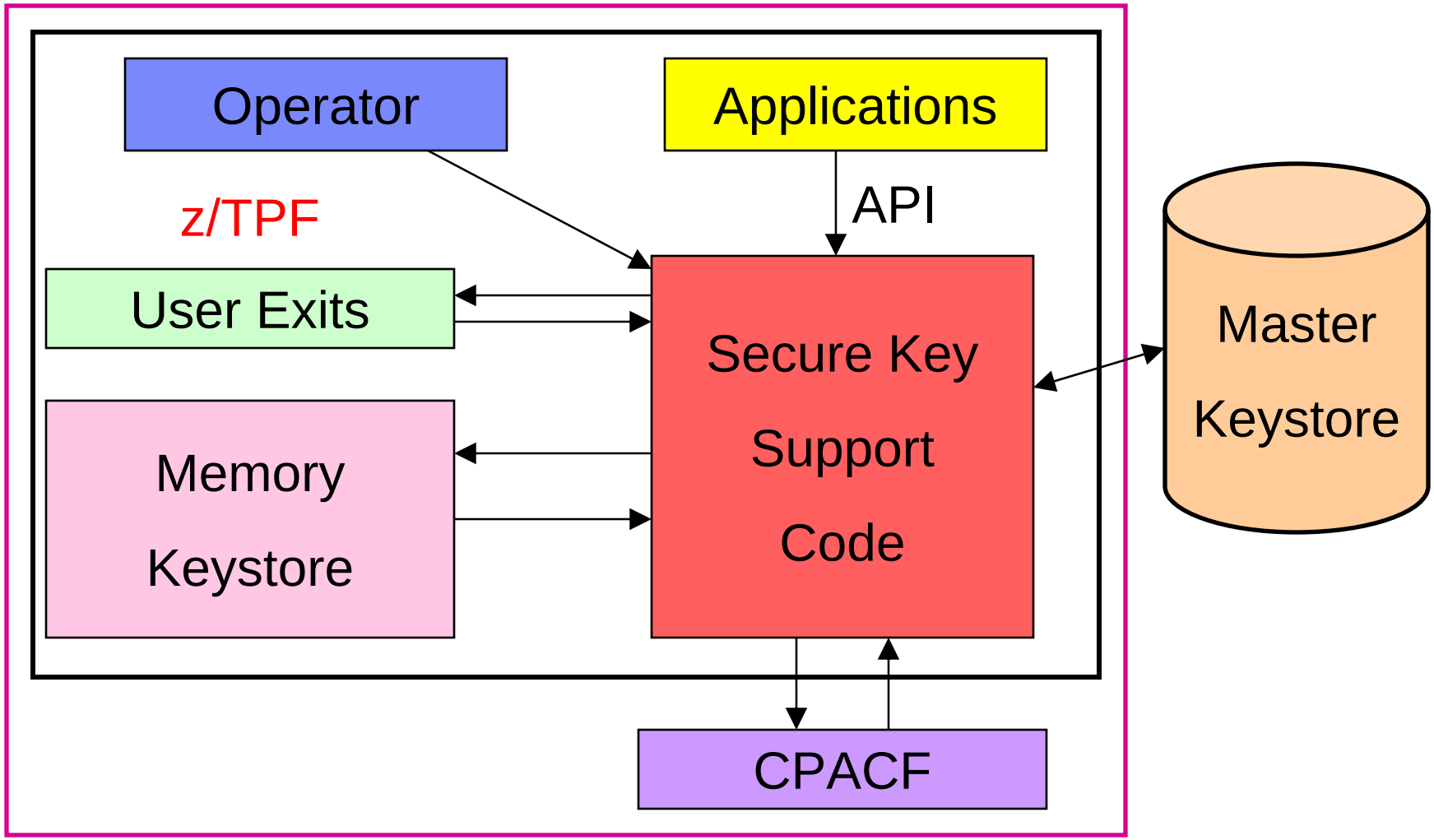
Name: Mark Gambino
Venue: Communications Subcommittee

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Secure Key Management Support

- **z/TPF APAR PJ31450 that shipped in 2007**
- **Enables you to create and manage symmetric encryption keys in a secure manner**
- **Applications can use the support to protect sensitive data stored on tape or disk (data at rest) or flowing over the network (data in flight)**
- **High performance designed for mainline application use**
- **Access controls to limit and log key usage**
- **Can help you meet the ever growing list of security and compliance standards**

Secure Key Support Component View



Secure Key Components

- **Master Keystore**
  - Persistent copy of encryption/decryption keys on DASD
  - Shared by all processors in the complex
- **Memory Keystore**
  - Copy of the master keystore information in memory on each CPU
  - Exists for performance reasons
- **Operator Interface**
  - Commands to create/activate/change keys, display keystore information, backup/restore keystore information
- **Application Interface**
  - APIs to encrypt and decrypt data using secure keys
  - API to add a key to the keystore
- **User Exits**
  - Control and log key usage (encrypt/decrypt data APIs)
  - Control and log keystore adds (add key API)

Original Secure Key Management Support

- **APAR PJ31450 provides support the following ciphers:**
  - DES and Triple-DES (TDES)
    - In regular or cipher block chaining (CBC) mode
    - Supported on z990 or higher
  - AES-128
    - In regular or cipher block chaining (CBC) mode
    - Supported on z9 or higher
      - CPACF on z9 added AES-128 support

Enhanced Secure Key Management Support

- **New APAR PJ32630**
- **Adds AES-256 support:**
  - In regular or cipher block chaining (CBC) mode
  - Supported on z10
    - CPACF on z10 added AES-256 support
- **Many security agencies and industry experts recommend using AES rather than TDES**
  - AES-256 is the preferred (stronger) version of AES compared to AES-128

Secure Key API testing with one CPACF using TDES

Data Size	z10 operations/second	z10 ratio versus z9
16	675,595	1.53
32	652,861	1.52
64	607,650	1.52
256	444,172	1.43
1024	212,432	1.34
4096	69,047	1.28
32,768	9,388	1.26
65,536	4,720	1.26
1,048,576	298	1.26

Tests performed on z10 and z9 – your results may vary

Secure Key API testing with one CPACF using AES-128

Data Size	z10 operations/second	z10 ratio versus z9
16	686,466	1.59
32	680,201	1.61
64	666,841	1.63
256	590,168	1.83
1024	414,887	2.19
4096	188,678	2.72
32,768	30,372	3.10
65,536	15,427	3.10
1,048,576	986	3.15

Tests performed on z10 and z9 – your results may vary

Secure Key API testing with one CPACF using AES-256

Data Size	z10 operations/second
16	686,431
32	677,960
64	660,546
256	571,500
1024	378,627
4096	160,350
32,768	24,780
65,536	12,556
1,048,576	798

Tests performed on z10 - your results may vary

Hardware Acceleration for SSL AES-256 Ciphers

- **z/TPF supports AES ciphers to encrypt/data data flowing over SSL sessions**
- **APAR PJ32630 also adds hardware acceleration support for SSL sessions that use AES-256**
  - If z/TPF is running on a z10, CPACF hardware is now used to encrypt/decrypt data on SSL sessions that are using an AES-256 cipher
  - If z/TPF is not running on z10, AES-256 operations continue to be performed via software encryption

Original Secure Key Delete Restriction

- **Original secure key management support did not allow you to delete a key if that key was ever used**
- **This was done to prevent loss of data**
  - If data was encrypted with this key and later on you need to decrypt this data, the data is unusable if the key has been deleted
- **You could deactivate the key to prevent it from being used to encrypt any new data, but the key is still available to decrypt data**

New Secure Key Delete Capability

- **Some customers indicated that despite the risks, their security auditors require old keys to be deleted**
- **New APAR PJ32687 provides this capability**
  - Optional FORCE parameter on ZKEYS DELETE command
  - You cannot delete a currently active key, even with the FORCE option
    - You must deactivate the key before deleting it
  - Because of the risks associated with deleting keys that were active (used) in the past
    - The FORCE option can be issued only from prime CRAS

Statement of Direction – PKI Support

- **Ability to create/manage RSA key pairs on z/TPF in a secure manner, similar to how existing secure key management support handles symmetric keys**
  - RSA private keys would be protected via the keystore
- **Ability to create digital certificate requests**
  - Using z/TPF generated RSA public key as input
- **Enable SSL applications to use z/TPF generated RSA key pairs**
- **Secure key import**
  - Ability to import a symmetric key in a secure manner from a remote key manager using RSA key wrapping
- **APIs to encrypt/decrypt data using RSA keys**
- **APIs to create/verify digital signatures**

Trademarks

- IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.
- Other company, product, or service names may be trademarks or service marks of others.

- Notes
- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

- This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.