z/TPF V1.1

2013 TPF Users Group

Hardware Cryptography and z/TPF

Mark Gambino
Communications Subcommittee

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

Overview of Current Support on z/TPF

Types of Hardware Cryptography on System z

- **Central Processor Assist for Cryptographic Functions (CPACF)**
  - Coprocessor integrated into the multi-chip module (MCM)
  - Each CPACF is shared by 2 cores
- **Crypto Express**
  - Physical cards that you plug into the processor
  - 1 feature = 1 physical card
    - 1 Crypto Express3 feature = 2 Crypto Express3 adapters
      - Each adapter operates independently
    - 1 Crypto Express4S feature = 1 Crypto Express4S adapter
  - zEC12 supports Crypto Express3 and Crypto Express4S

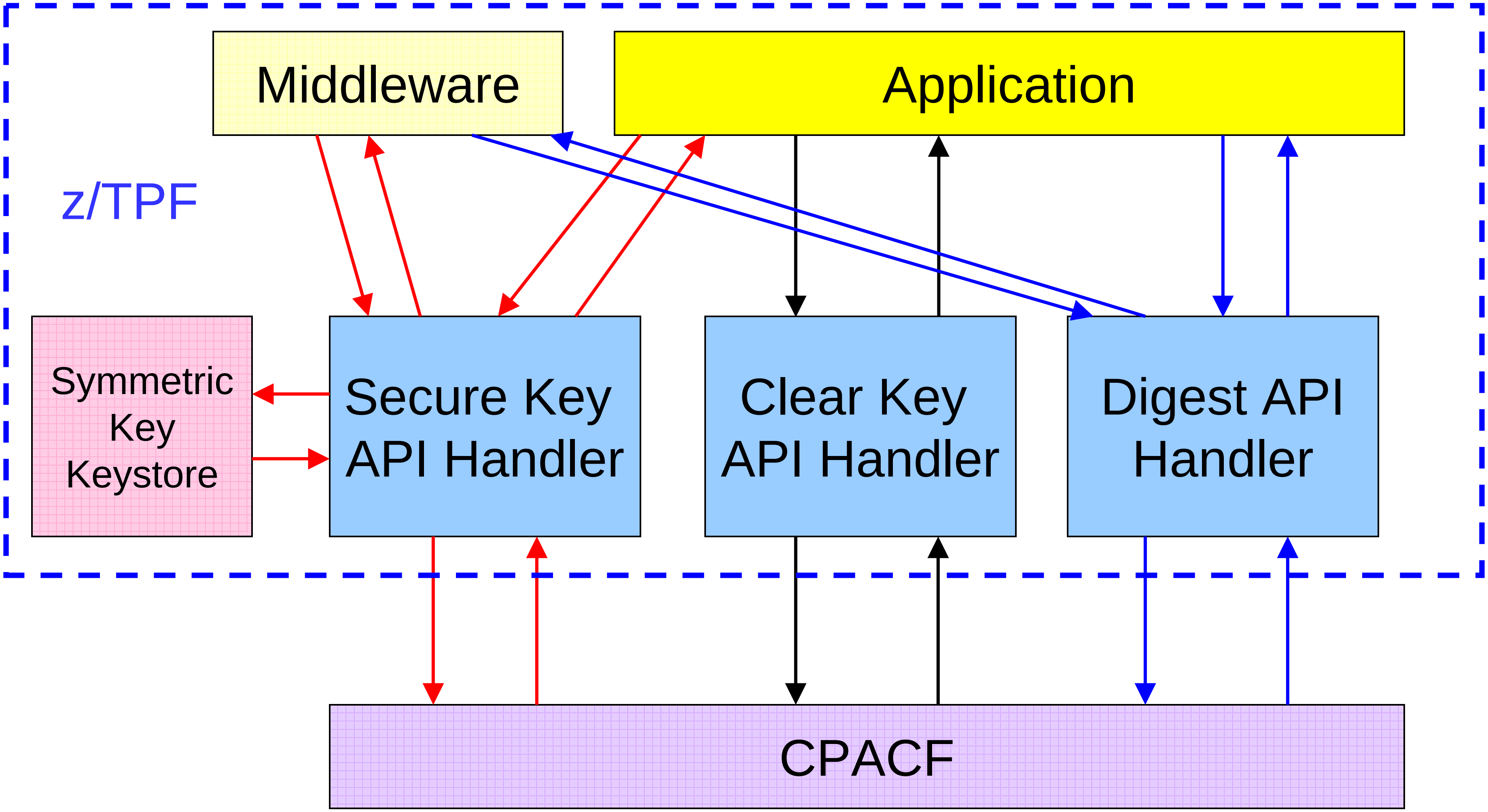
Basic z/TPF Crypto Support

- **Clear key APIs**
  - Encrypt/decrypt data using DES, TDES, AES-128, or AES-256
    - Uses CPACF if the algorithm is supported by CPACF on the processor; otherwise, software is used
  - Key management is user responsibility
- **Digest APIs**
  - Create/verify digest of data using SHA-1 or SHA-256
  - Requires that the CPACF on the processor supports the algorithm

Secure Symmetric Key Management Support

- **Enables you to create and manage symmetric encryption keys in a secure manner**
  - DES, TDES, AES-128, and AES-256
  - Requires that the CPACF on the processor supports the algorithm
- **APIs to enable applications to protect sensitive data**
- **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**

z/TPF Symmetric Key Cryptography and Digest APIs



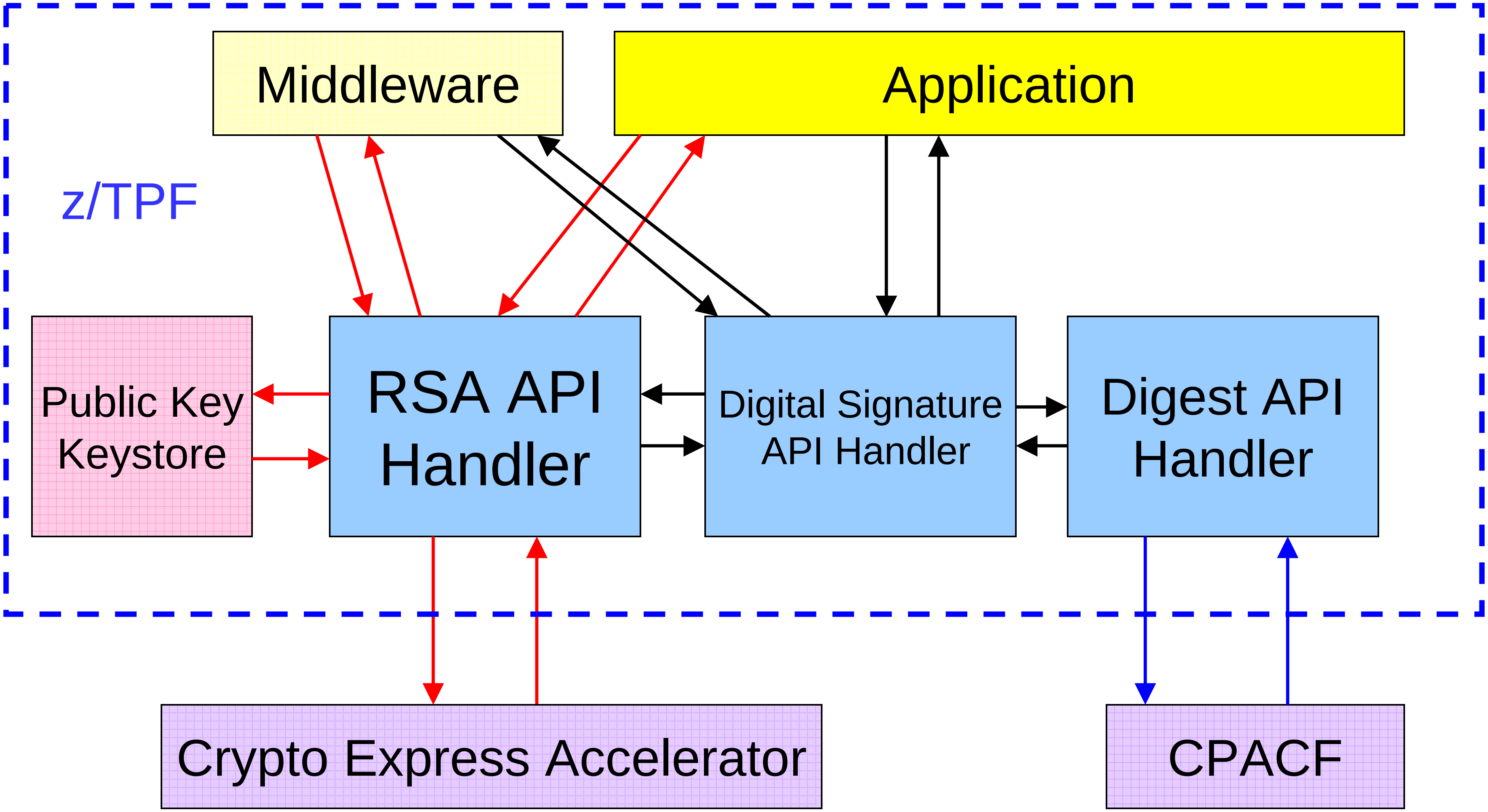
z/TPF Public Key Infrastructure (PKI) Support

- **Create and manage RSA public key pairs in a secure manner on z/TPF**
- **Use the RSA keys generated on z/TPF to create digital certificate requests as well as self-signed digital certificates**
- **Enable z/TPF SSL applications and middleware to use private keys generated by z/TPF**
- **APIs to encrypt and decrypt user data using RSA**
- **APIs to create and verify RSA digital signatures**

Crypto Express Accelerators

- **Crypto Express adapters can be configured to run in different modes**
  - An adapter runs in only one mode at a time
- **Crypto Express adapter running in accelerator mode performs RSA operations at a high rate**
  - Up to a few thousands operations per second depending on the operation type and key size
- **Required to use z/TPF PKI support**
- **Recommended to use SSL support**

z/TPF Public Key Cryptography



Crypto Express Coprocessor

Crypto Express Coprocessor

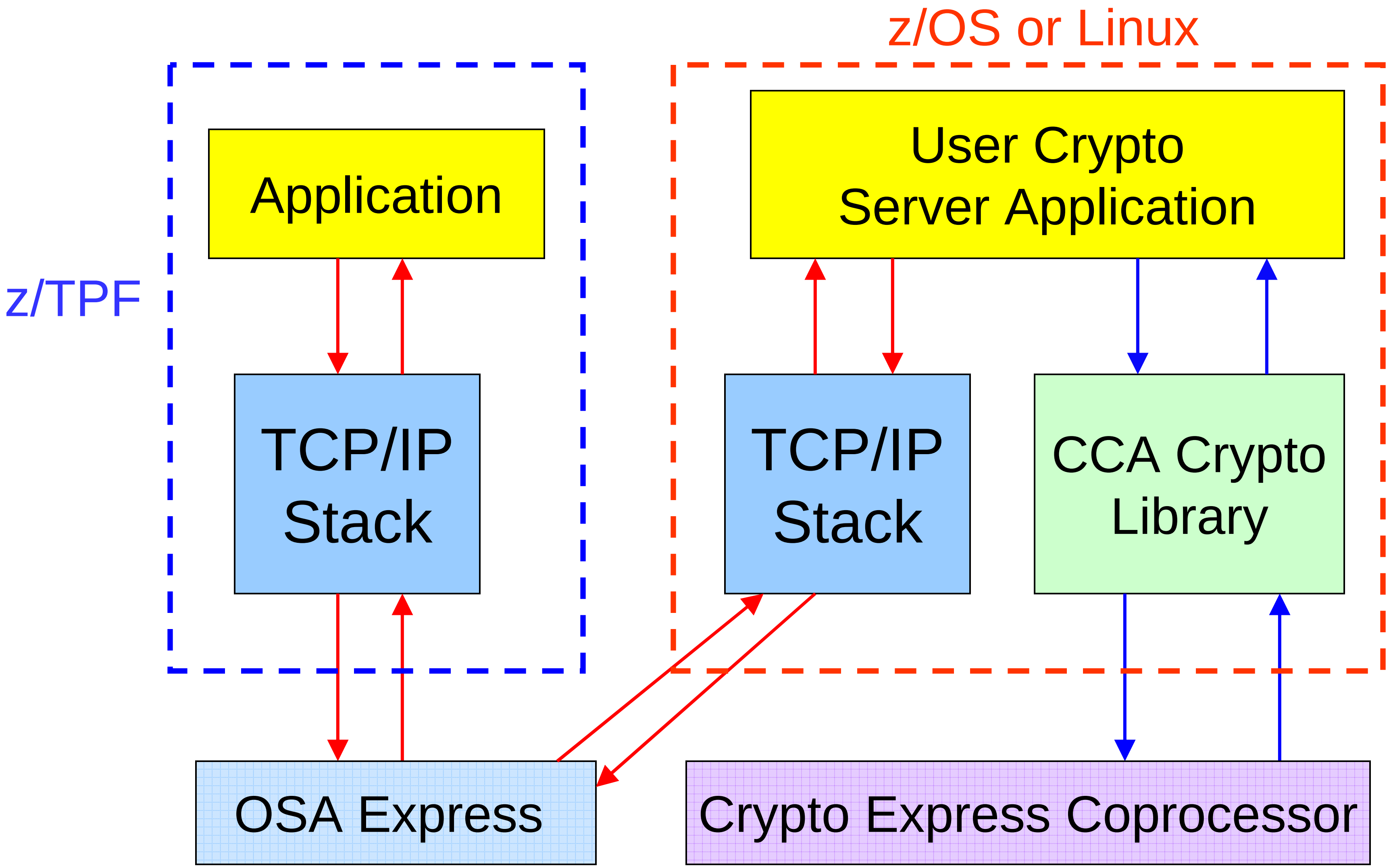
- **Crypto Express adapters can also configured to run coprocessor mode**
  - Supported by z/OS and Linux on z
  - Not currently supported by z/TPF
- **IBM Common Cryptographic Architecture (CCA)**
  - APIs support many algorithms, including banking cryptography functions
- **Customer loads master keys into the adapter using a secure trusted key entry (TKE) interface**
  - Secure, tamper-resistant card
  - FIPS 140-2 level 4 certification
- **A user key needs to be encrypted under the master key to become an operational key**

Using Another LPAR to Access Crypto Express Coprocessor

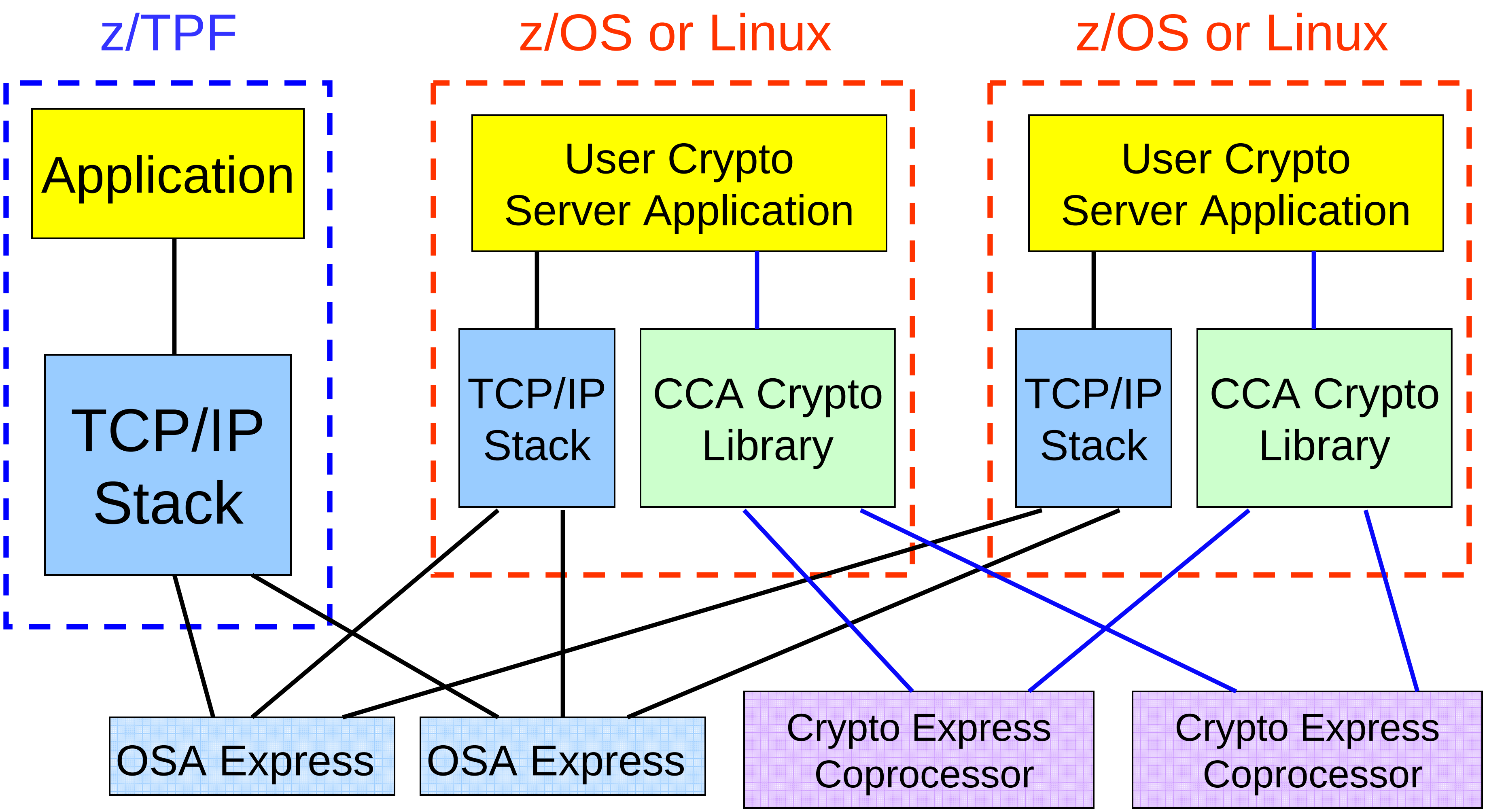
- **If you have z/OS or Linux LPARs, today you could use those LPARs to access Crypto Express coprocessors**
- **How to do this:**

1. Update your z/TPF application to send a message over TCP/IP to the other LPAR
   - Message contains the name of the CCA API along with all the input parameters to that API
2. Write a server program on the other LPAR that receives the message from z/TPF over TCP/IP, issues the appropriate CCA API, then passes the output of that API back to the z/TPF application over TCP/IP

Using Another LPAR to Access Crypto Express Coprocessor



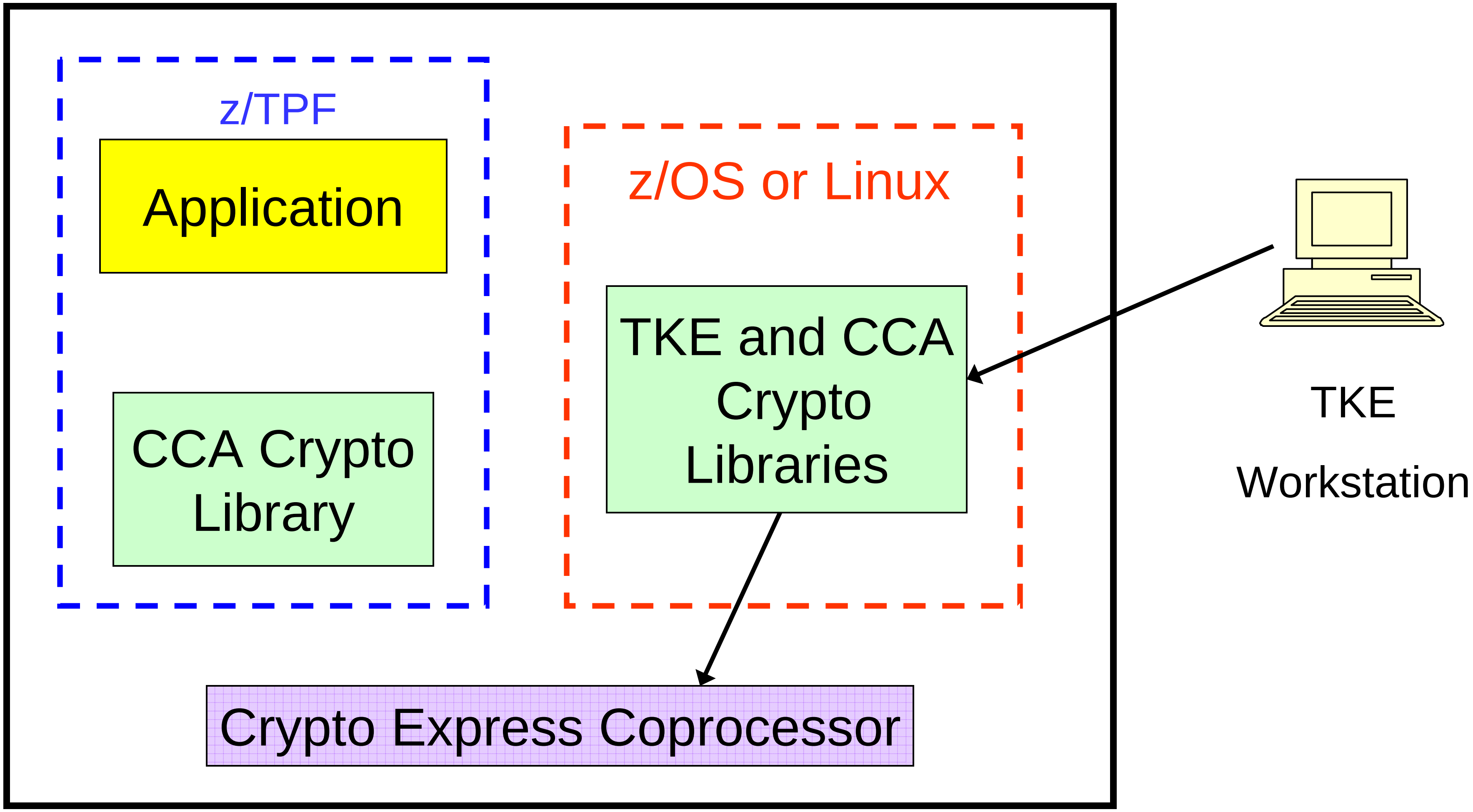
Using Another LPAR to Access Crypto Express Coprocessor High Availability Configuration



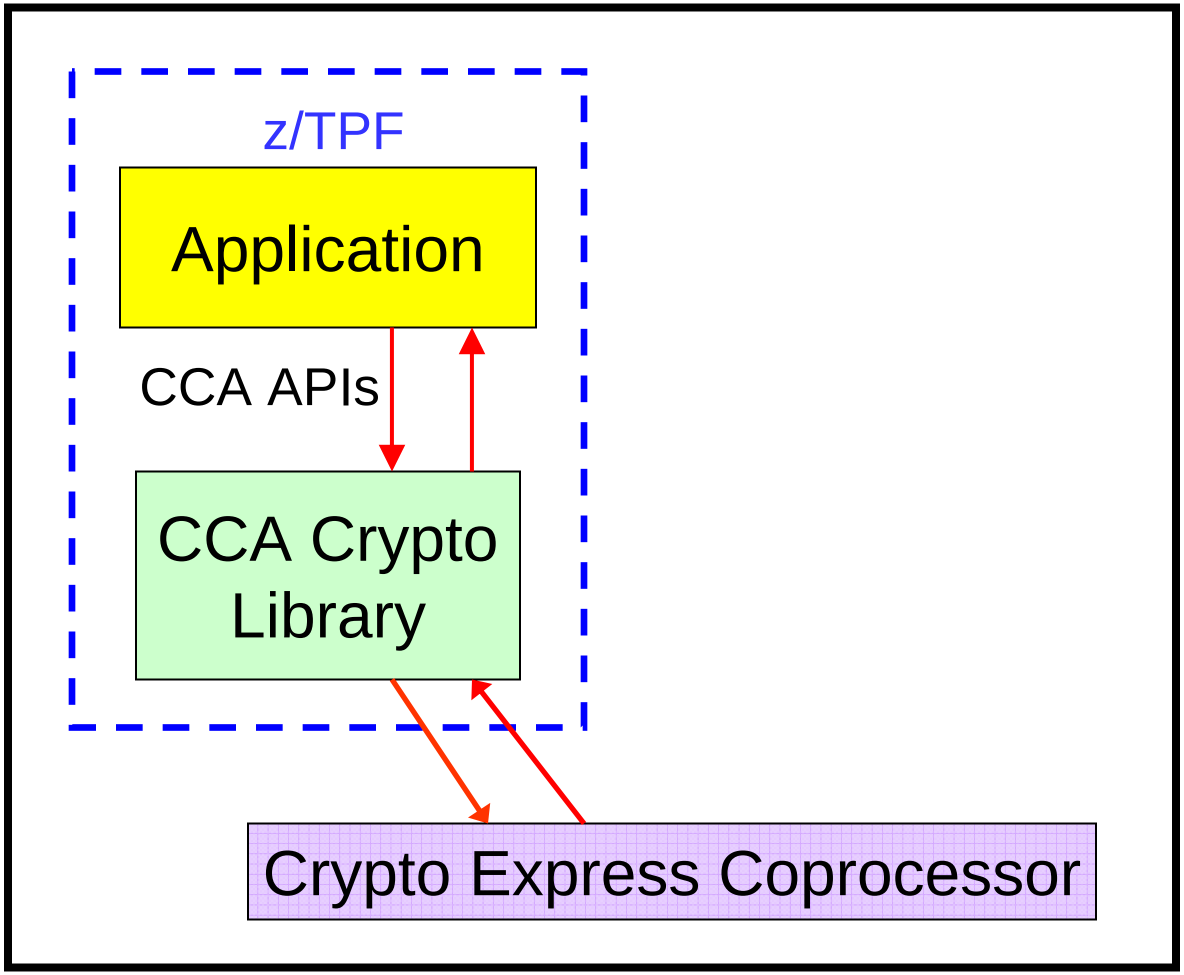
Any Interest in z/TPF Supporting Crypto Express Coprocessor Directly?

- **Port portions of the CCA library from Linux to z/TPF**
- **Need to know which APIs you want z/TPF to support**
  - **http://www.ibm.com/security/cryptocards/pciecc/pdf/SC33-8294-03.pdf** defines the APIs available on Linux for System z
  - These APIs are also implemented by the Integrated Cryptographic Service Facility (ICSF) on z/OS
- **Also need to know what options on each API you plan to use**
  - For example, some APIs have dozens of different options
- **Need to know what key management APIs you would need**
  - Creating keys, importing keys, changing master keys
- **Would need a z/OS or Linux LPAR on the processor where the Crypto Express coprocessor resides to load or change master keys on that adapter**

z/TPF with Some Crypto Express Coprocessor Support: Loading Master Keys



z/TPF with Some Crypto Express Coprocessor Support: Applications Issuing Crypto APIs



Options for Crypto Express Coprocessor Use by z/TPF

1. **Do nothing – no interest in Crypto Express coprocessor**
2. **Customer written code to access Crypto Express coprocessor on another (z/OS or Linux) LPAR**
   - IBM could provide client communications layer to do server selection, load balancing, and exchange messages with the selected server
     - This code could be general purpose for exchanging any type of user message between a z/TPF client and one of many servers
3. **z/TPF supports a limited subset of the CCA APIs to access Crypto Express coprocessor directly**

Trademarks

- IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
- *(Include any special attribution statements as required – see Trademark guidelines on https://w3-03.ibm.com/chq/legal/lis.nsf/lawdoc/5A84050DEC58FE31852576850074BB32?OpenDocument#Developing%20the%20Special%20Non-IBM%20Tr)*

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.