zSeries Crypto Migration Considerations

IBM Advanced Technical Support

First Things First

- What You Should Know
- Installation Changes You Should Be Aware of
- z990/890
  - This isn't the same as the previous crypto hardware!!
- ICSF Migration
- Application Migration

First Things First . . .

- Hardware Crypto use is dictated by the specific crypto call made within an application
- Application code will drive all crypto function
  - Become familiar with the ICSF Application Programmer's Guide Chapters 1 - 3
  - CSNxxxxx callable services and the new MSA instructions are routed to specific crypto hardware features
    - Routing can be influenced by parameter usage
- Hardware, keys, ICSF, key data sets, master keys, are all related
- Nothing is ever a simple answer

What You Should Know

- Everything!
  - Crypto Technology
    - Things like parity....
    - Things like variants...
  - Crypto Related Standards
    - IETF
    - Certificates, etc.
  - IBM Crypto Concepts (Common Crypto Architecture)
  - IBM Product Details
- READ! READ! and READ some more!!!!
  - Research web articles
  - Learn how to find info
- ATS TechDocs
- IBM Web Library and Product Sites

What You Should Know . . .

- Crypto Systems consist of
  - Engines that perform the mathematical processes needed
  - Keys
  - Application Programming Interfaces (APIs) or callable services
- Crypto decisions should not be made be anyone who does not understand
  - The environment in which it will be used
  - The application requirements
  - Key management issues
  - The crypto system to be used
- Crypto isn't hard but it does demand a level of comprehension and knowledge

zSeries and Total Storage Update (zSTSU)

What You Should Know . . .

- Common protocols
  - SSL, Secure Sockets Layer
    http://wp.netscape.com/eng/ssl3/ssl-toc.html
  - TLS, Transaction Layer Security
    http://www.ietf.org/html.charters/tls-charter.html
  - IPSec
    http://www.ietf.org/html.charters/ipsec-charter.html
- Not understanding the protocols and how crypto is/could be used within the protocol leads to unanswered questions and misunderstandings
- Read the protocols!!
  - Comprehend them
  - Consider how the crypto functions within the protocol might be performed on IBM Crypto hardware, which features

What You Should Know . . .

- Keys and their values are highly security sensitive items
- If values are not protected, no encryption algorithm can really protect the data
- Do not throw away key data sets
  - CKDS can always be brought forward across releases AND master key changes
  - Almost never a need to initialize a new CKDS once a CKDS has been created
- TPF is an operating system that does not have an IBM Crypto driver nor can it use ICSF
- Following step-be-step directions to use crypto is not due diligence if you do understand enough to make decisions
- IDCAMS REPRO used secure services - clear keys were imported (encrypted) before use

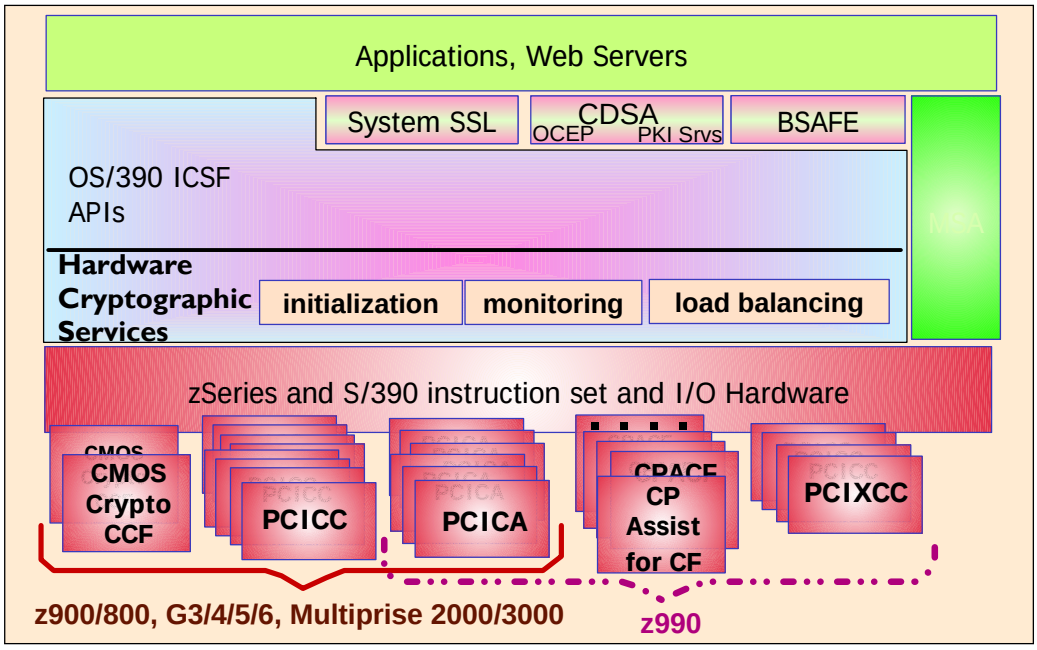
What Should be Read

- ATS TechDocs search with keyword of crypto
  - Many documents concerning crypto
  - Read at least 3 of any relevant papers
  - Check out all relevant flashes
- Read the latest ICSF pubs
  - ICSF is in the z/OS Crypto Services bookshelf in z/OS basic
  - ICSF System Programmer's Guide
    - Summary of Changes
    - Appendices
    - Migration Chapter
  - ICSF Application Programmer's Guide
    - Appendices
    - Summary of Changes
  - ICSF Administrator's Guide
    - Note any changes

Relationships

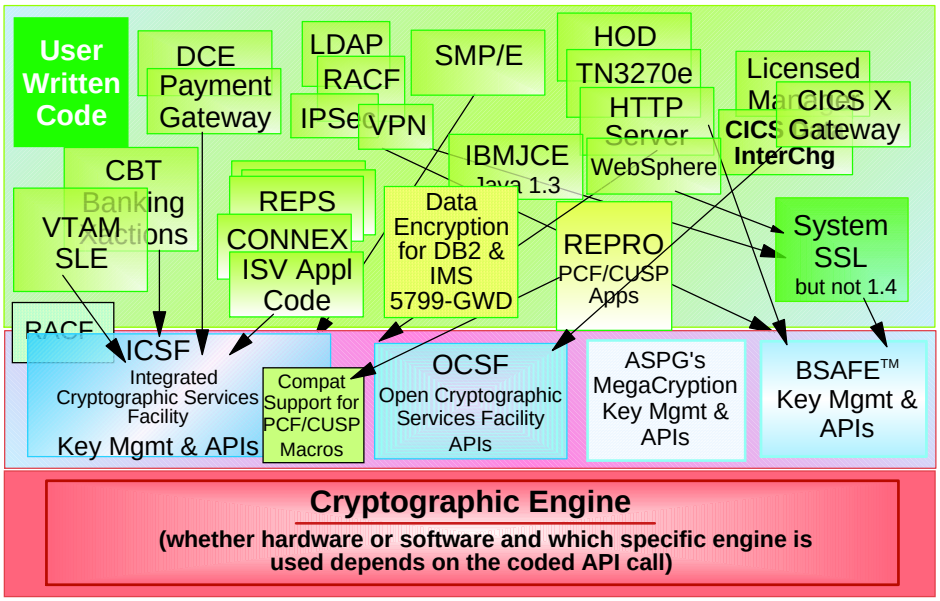
- Crypto hardware to processor
- Crypto hardware definitions to LPAR usage
- Crypto hardware definitions to ICSF Options data set
- Crypto hardware definitions to key value processing within LPAR
  - Crypto master key storage
- Master keys to key data sets
- Configuration data to usage capabilities
- Domain assignments to usage by LPARs
- Key token contents to
  - Master Keys
  - Usage
- Application coded request to hardware feature required/used

Access to Crypto Hardware



Access to Crypto Hardware . . .

Application design & code determines which crypto engine will be used and when.



Installation Changes You Should Be Aware of

- ICSF code may have updates that add support so check for web deliverables
  - http://www-1.ibm.com/servers/eserver/zseries/zos/downloads
- Check PSP bucket for information on APARs and MCLs
- When sharing a CKDS with CCF systems and the IBM eServer zSeries 990, the CKDS must be created on a CCF system.
- CKTAUTH is a new ICSF Option whether to authenticate each record read from CKDS.
- Beginning with HCR770A, the PKDS must be initialized.
- CSFDPKDS must be added to PARMLIB(IKJTSOxx) member's AUTHCMD and AUTHTSF lists
- PKDS, Public Key Data Set, must be initialized in HCR770A
  - No RSA keys stored, no problem - initialize from screen
  - RSA keys stored, work to be done

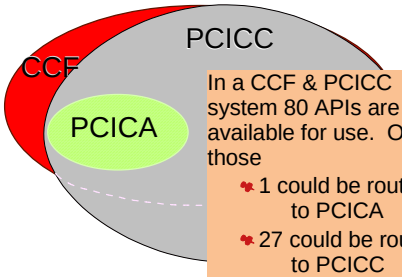
z990/890 Crypto Hardware Changes

- CPACF is
  - The base integrated crypto feature in z990
  - NOT the same functionality as CCF
- CPACF does NOT perform the functions that would have been used by most applications in a CCF environment
  - Only a small subset of functions are done by CPACF that were done by CCF
  - SHA-1 is available on CPACF and is available without enabling CPACF with configuration load
  - CSNBENC / CSNBDEC for data privacy are not available on CPACF
  - CSNDPKE / CSNDPKD and CSNDDSV are not available on CPACF
    - These are the APIs that boost SSL performance in a CCF environment
    - That boost is lost in a CPACF only environment

z990/890 Crypto Hardware Changes . . .

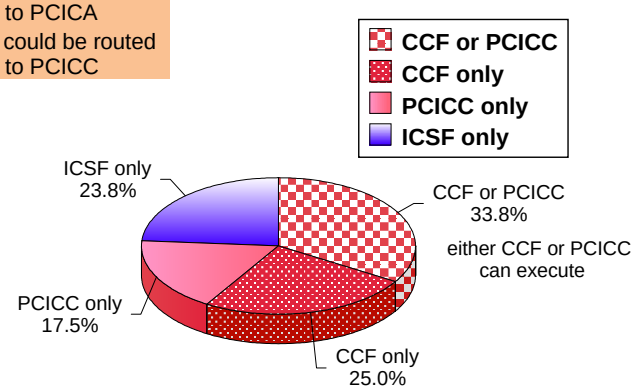
- The loss of function in a CPACF only environment is the BIGGEST driver of problems in a z990/890
  - Effects SSL usage
  - Effects ISV usage
- The other problem affecting migration with crypto hardware changes is determining whether crypto is available
  - Use of CCFT field, CCVTSFG1, causes problems when used for checks on crypto availability
    - Not a customer defined interface
    - Therefore, not guaranteed to work the same way across releases
    - Having said that, the CCVTMK bit (Bit 1 of CCVTSFG1) in this field is a good indicator for both secure features
  - This field dealt with CCF primarily, but the MK bit is also set for PCIXCC
  - CSFICQ is a new HCR770A utility callable service allowing queries on crypto status

API Comparison for 1st Generation Hardware



In a CCF & PCICC system 80 APIs are available for use. Of those
- 1 could be routed to PCICA
- 27 could be routed to PCICC

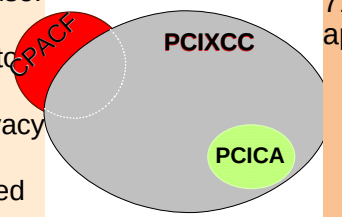
In a CCF system 66 APIs are available for use. Of those
- 1 could be routed to PCICA



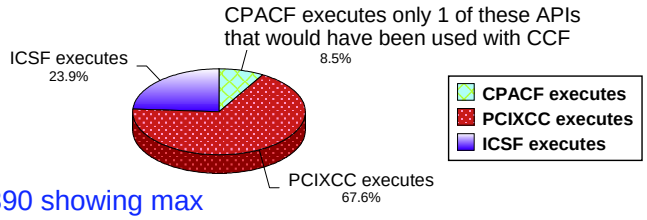
9672 - z900 showing max API capability by HW

API Comparison for 2nd Generation Hardware

In a CPACF system 14 APIs are available for use. Of those
- 6 could be routed to CPACF
- None are data privacy from earlier APIs
- 8 are ones executed by ICSF

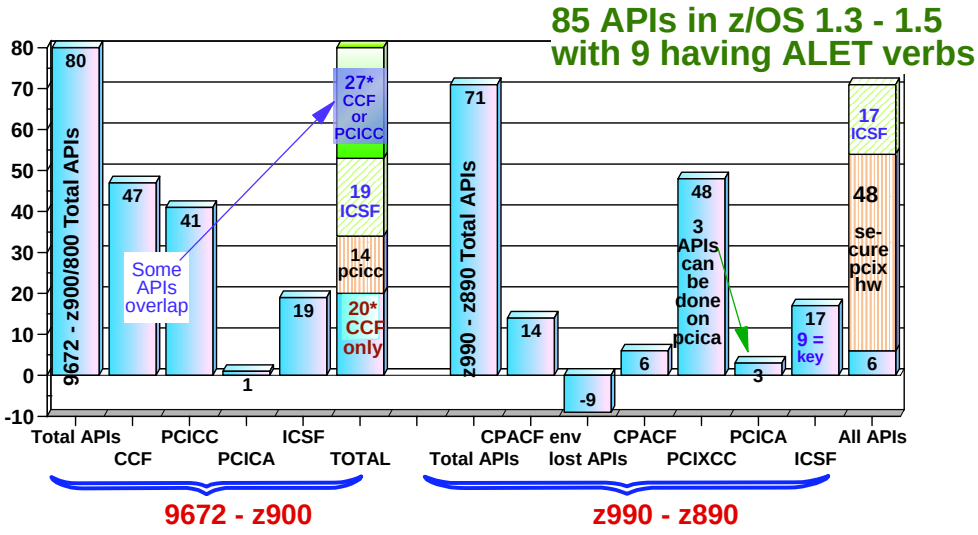


With PCIXCC in the system 71 APIs are available for application requests.
- 17 are ones executed by ICSF
- 6 are those for CPACF
- 48 APIs provide support from CCF and PCICC environments
- 9 APIs are no longer supported



z990 - z890 showing max API capability by HW

API Comparison Across Crypto Environments



Hardware Usage & Performance

- PCIXCC is not as fast as CCFs for data privacy using secure key but can be comparable for certain functions
- CPACF is fast as CCF for data privacy but use must be balanced with data risk assessment for clear key
- CPACF and PCICA without PCIXCC cannot do many of the crypto functions that previous applications (non-SSL) running on z900/800 and below required
- Crypto Express2 will have function of PCIXCC and RSA processing speed of PCICA

Crypto Application Migration Issues

- Be aware of which application programming interfaces are used by applications
- MSA instructions leave no trail in object code
  - No way to check for KM or KMC use
  - CPACF may not be available when needed in a mixed processor environment or Disaster Recovery
- Disaster Recovery Impact
  - If MSA is used to encrypt data, the key value must be available if data is required to be restored on a non z990 system
  - DR sites should have IBM crypto hardware required for the functions critical to production applications
    - API requiring a specific feature will fail, if feature not available
    - If requests that only execute in a secure hardware environment are required the master key values used to protect the Key Data Sets to be used in DR must be loaded into the DR crypto hardware

zSeries Applications Exploiting Crypto Hardware

- Generally the exploitation is for improvement of RSA function
  - SSL - the decrypt/encrypt of a symmetric key value using a clear key value stored external to ICSF data sets
  - IPSec - data privacy
  - Very CPU-intensive operations
- Some exploitation of new CPACF for clear-key encrypt/decrypt
  - Very little via the hardware instruction set
  - Has impact to operational conditions
- z/OS and OS/390 Application Crypto software products
  - System SSL
  - Open Cryptographic Services Facility (CDSA APIs for applications)
  - PKCS 11 Toolkit
  - Cryptographic Drivers for Linux and Java

Interface to Crypto Hardware on Other Mainframe OSs

- z/VM
  - With z/VM 5.1.0 (GA 8/04) VM supports PCIXCC, PCICA & PCICC for z/OS guests
    - Dedicated queue support for clear-key & secure-key functions, i.e. specific to a z/OS LPAR
    - Shared queue & dedicated queue support for clear-key functions, for Linux on zSeries with up to 256 dedicated queues, i.e., no unique data
- Open Source for use by Linux and UNIX
- TPF
  - none

zSeries and Total Storage Update (zSTSU)

Questions?

z9XX Crypto | MarilynAllmond | Wahington Systems Center
© 2004 IBM Corporation