IBM

zSTSU 2004
Ordering Crypto:
What You Need to Understand

Greg Boyd
December 8, 2004
IBM Washington Systems Center
Advanced Technical Support
Gaithersburg, MD
boydgy@us.ibm.com

1

IBM

After Jan 29, 2005 there is an Easy Answer

z890/z990

CPACF

Crypto Express2 $e_{mk}(k)$

2

IBM

The Hard Answer Is …

- z890/z990 prior to January 29, 2005
  - CPACF
  - PCICA
  - PCIXCC *
  - or both (PCICA & PCIXCC)
- z800/z900/G6
  - CCF*
  - PCICC *
  - PCICA
  - Or both (PCICA and PCICC)

*denotes secure key - $e_{mk}(k)$

3

IBM

Clear Key vs Secure Key

- Clear Key
  - c'MYDATAKY' or x'D4E8C4C1E3C1D2E8'
- Secure Key
  - e_{mk}(MYDATAKY) = C'9*B! @1r'
  - $e_{kek($(MYDATAKY) = C'w$& L c('

4

IBM

So the First Decision Is …

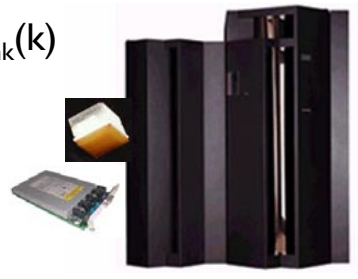
- Secure Key or
- Clear Key or
- Both

5

IBM

z890/z990 Features

- 3863 CPACF DES/TDES Enablement
- 0862 PCICA
- 0863 Crypto Express2 $e_{mk}(k)$
- 0868 PCIXCC $e_{mk}(k)$



6

IBM

z800/z900 Features

- 0800 Crypto $e_{mk}(k)$
- 0861 PCICC $e_{mk}(k)$
- 0862 PCICA
- 0865 T-DES for PCI Crypto
- 0867 T-DES for PCI Crypto-2048 Bit
- 0875 T-DES w/TKE

7

IBM

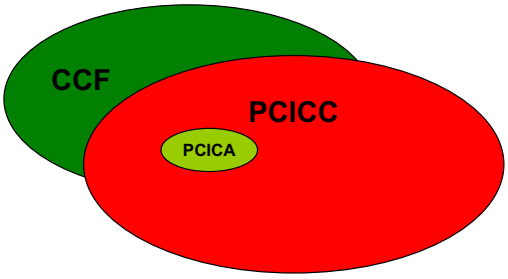
G6 Features

- 0800 Crypto Coprocessor Hardware Feature
- 0835 T-DES with PKA & TKE
- 0865 TDES w/PKA
- 0860 PCI Cryptographic Coprocessor $e_{mk}(k)$

8

IBM

Hardware functions overlap on the z800/z900



On a CCF Only system, 66 APIs are available

With a CCF & PCICC, 80 APIs are available

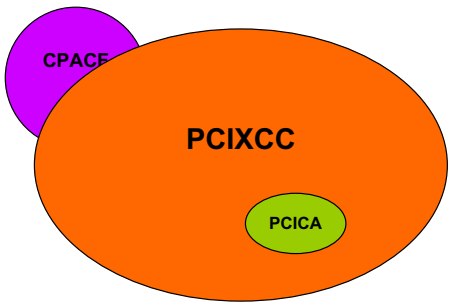
PCICA only supports a single API

Shamelessly copied from Marilyn Allmond's foils

9

IBM

Hardware functions overlap on the z890/z990



On a CPACF Only system, 14 APIs are available (6 are routed to the CPACF and 8 handled by ICSF)

With a PCIXCC, 71 APIs are available

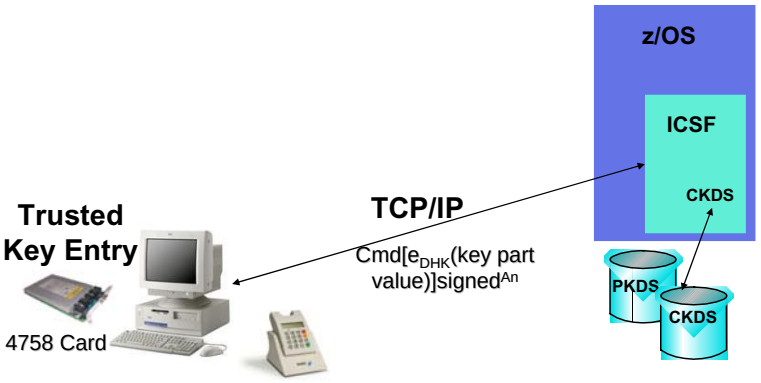
PCICA supports 3 APIs

Shamelessly copied from Marilyn Allmond's foils

10

IBM

To TKE or not to TKE …



11

IBM

TKE Features on z800/z900 & z890/z990

- 0846 TKE 4.x with Token Ring
- 0849 TKE 4.2 with Ethernet
- 0853 TKE 4.2 Code
- 0887 TKE 4.2 Smart Card Reader
- 0888 TKE 4.2 Additional Smart Cards

12

IBM

TKE Features on G6

- 0846 TKE 4.x with Token Ring
- 0849 TKE 4.2 with Ethernet

- 0853 TKE 4.2 Code

13

IBM

Internal References

- ATS TechDocs – http://www.ibm.com/support/techdocs (then Choose Search All Documents, use keyword Crypto)
- Pubs
  - SA22-7519 ICSF Overview
  - SA22-7521 ICSF Administrator's Guide
  - SG24-6870 zSeries Crypto Guide Update
- Training/Installation Support
  - The ICSF Programming Workshop and S/390 & zSeries Crypto Hardware, ICSF, TKE Installation and Overview Workshop are now private workshops
  - Tailored training available thru ATS
  - Installation Services available thru ATS

14

IBM

External References

- Standards
  - http://www.ietf.org
  - http://www.itl.nist.gov/fipspubs/by-num.htm
  - http://csrc.nist.gov/cryptval/140-1/1401val.html
  - http://www.rsasecurity.com/rsalabs/
- Free Stuff
  - http://infosecuritymag.techtarget.com
  - http://www.scmagazine.com/home/index.cfm
  - http://www.counterpane.com

15