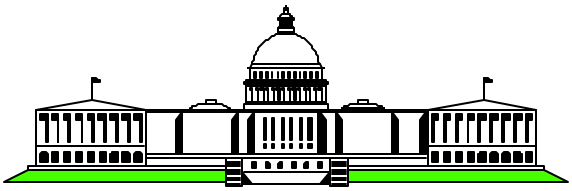
CMOS Crypto Overview



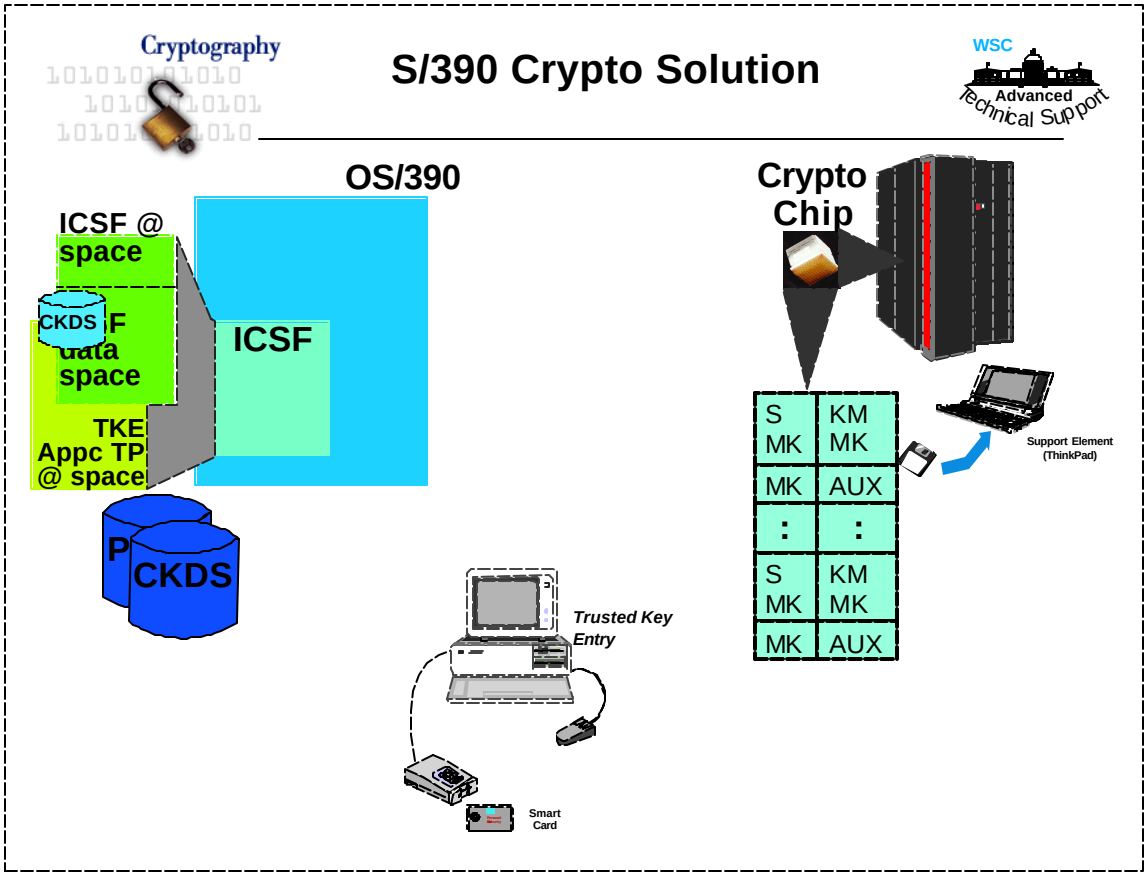
Washington Systems Center
Advanced Technical Support
S/390 Security

Marilyn Frazier Allmond

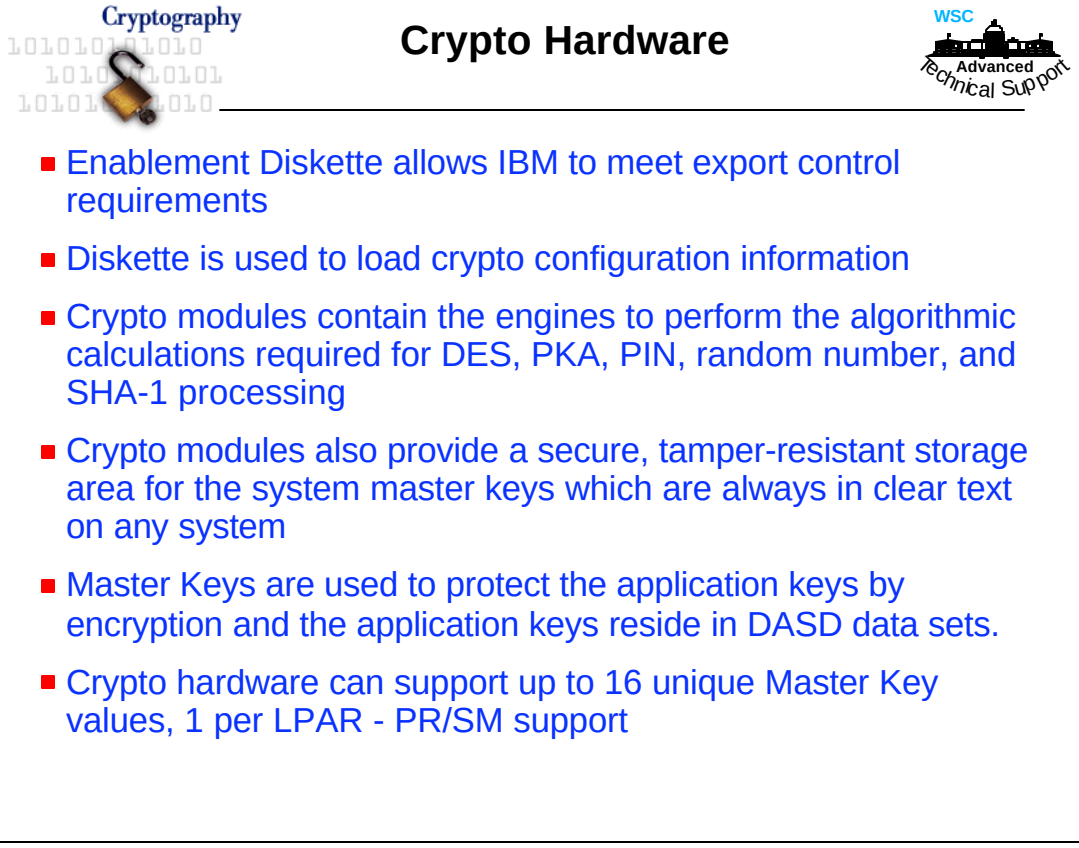
CMOS S/390 Crypto Solution

- CMOS Hardware - shipped with no active configuration
  - Enablement Diskette
  - Logical Partition
- OS/390 Integrated Cryptographic Services Facility
  - Customization
  - Key Entry
- Trusted Key Entry Workstation
  - Pentium PC, Monitor, Keyboard
  - OS/2 Operating System and associated applications
  - TKE application and its prerequisite applications
  - Optional Devices
    - Card Reader
    - Personal Security Card

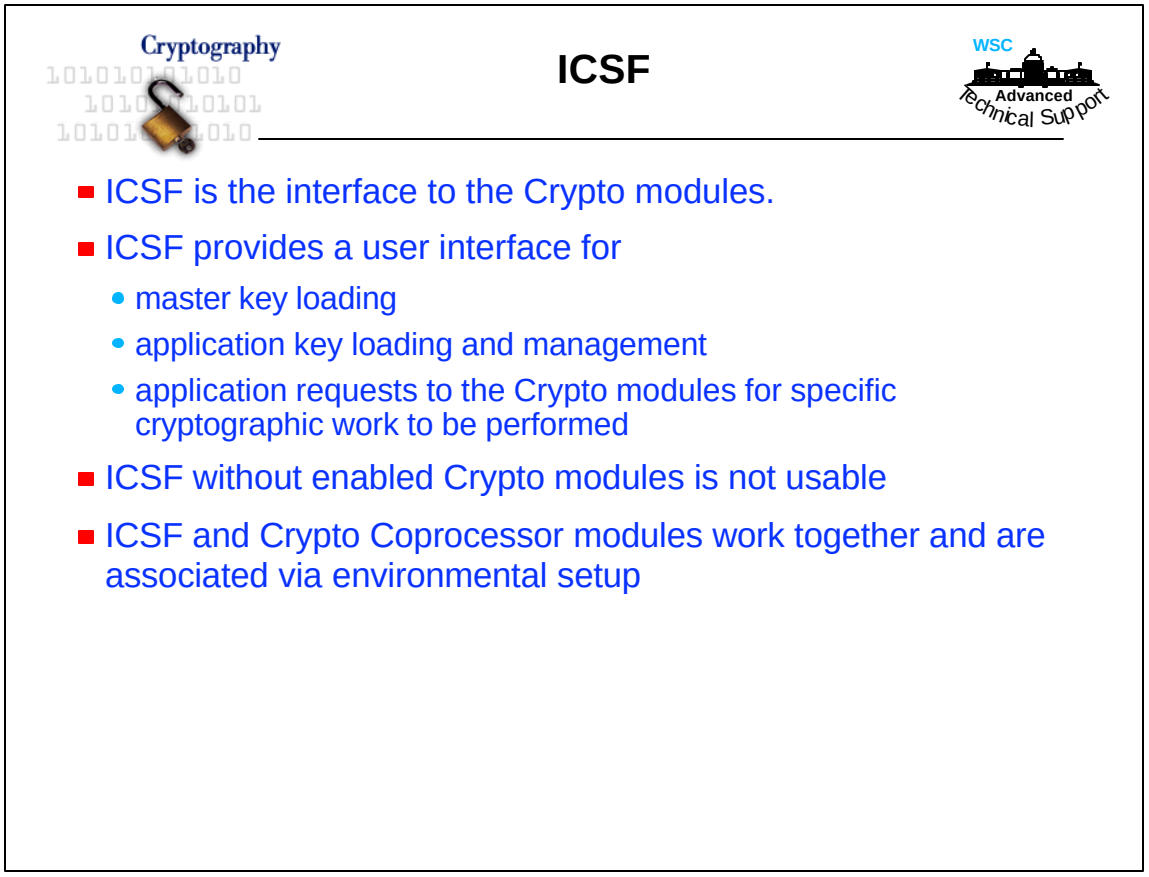
- The Crypto hardware is the Cryptographic Coprocessor. Associated with it is the Enablement Diskette which is the crypto 'LIC' ordered with the processor
- The configuration files that the Enablement Diskette loads are based on those choices you make when ordering the crypto 'LIC'
- The Enablement Diskette is 'linked' to the server by serial number. And, each configuration file on the diskette is linked to a specific cryptographic module.
- The loading of the Enablement Diskette is done by the IBM CE. The configuration files are stored on the Support Element. A POR/IML is required to have the files sent to the crypto modules. This process is referred to as 'activation'.
- The hardware contains the 'engines' to perform the mathematical functions required by the cryptographic algorithms and mechanisms
- Reference - Support Element Operations Guide
- The Crypto software is ICSF. ICSF and Crypto Coprocessor work together. Alone neither is usable.
- ICSF provides the interface to the Crypto hardware for
- loading of master keys both DES and PKA
- making application requests for cryptographic functions
- ICSF provides a management utility for DES application keys. API interfaces are available for the management of both DES and PKA application keys
- ICSF provides the interface to the VSAM key data sets for the storage of application keys.
- DES application keys are stored in the CKDS.
- PKA application keys are stored in the PKDS.
- ICSF runs as a started task and has an associated data space in which the CKDS is loaded.
- No crypto service or function is available from the crypto hardware until DES Master Key values have been loaded.
- The TKE is an optional, charged feature that provides
- A more secure key entry since the key parts loaded via the TKE are encrypted between the TKE and the Crypto Coprocessor.
- A more granular administrative interface to the Crypto hardware
- Ability to load key parts to the Crypto Coprocessor remotely
- Ability to generate RSA key pair



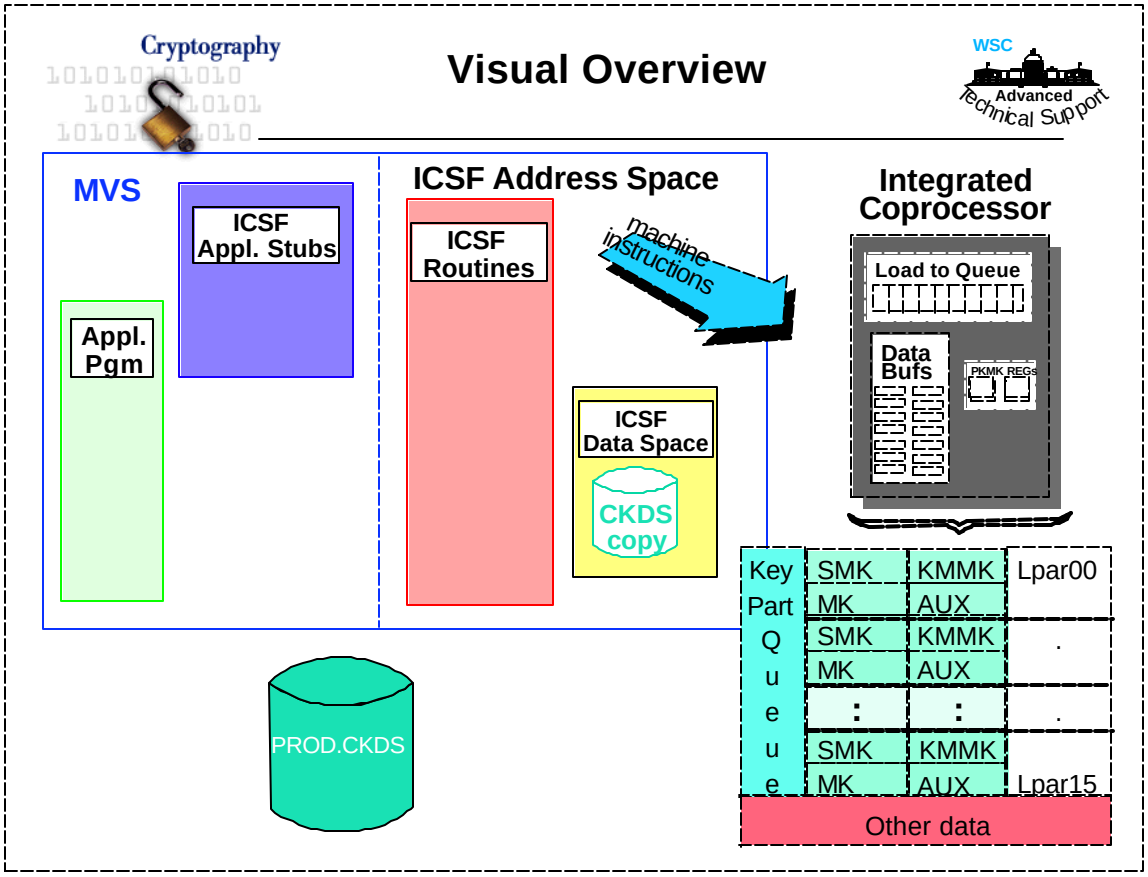
- To the right is a visual of the crypto hardware emphasizing these important points
- Crypto Coprocessor is integrated into the CMOS server. It is a part of the server not channel-attached.
- Each crypto chip supports PR/SM via the principal of crypto 'domains'. A domain is a storage area specifically for the crypto security data associated with a particular logical partition (LPAR). Think of this area as a table and each LPAR can be assigned a row within the table. In the visual 2 rows represent a LPAR association simply to prevent the table from being too wide.
- The 2 rows and 2 columns per LPAR illustrate that each LPAR can have a
- SMK - Signature Master Key used to protect PKA application keys designated as being used solely for digital signatures. This designation is done during the process of defining the PKA key to ICSF's standard format of keys called a token.
- KMMK - Key Management Master Key used to protect PKA application keys designated as being used either for protecting symmetric (DES or CDMF) keys during distribution or for digital signatures. This designation is done during the process of defining the PKA key to ICSF's standard format of keys called a token.
- MK - Master Key used to protect DES or CDMF application keys.
- AUX -Auxiliary Key is a place holder for the value associated with the a DES Master Key. The designation of this value can either be the New Master Key or the Old Master Key depending on the status of master key entry.
- Note the visual of the chip is a picture of an actual crypto coprocessor.
- The Enablement Diskette is shown with an arrow pointing to a representation of the Support Element. This refers to the loading process.
- To the left is a visual of the crypto software emphasizing these important points
- ICSF is a base component of OS/390 beginning with R4.
- ICSF has its own address space and an associated data space
- A complete copy of the disk CKDS is read into storage and placed in the data space. The size of the in-storage copy is limited by the max size of a data space
- If TKE is used, there will be a TKE Transaction Program running in the APPC address space on that MVS system.
- There are 2 key data sets shown underneath the ICSF visual. There is a DASD key-sequential data set for DES application keys, CKDS, and one for PKA application keys, PKDS.
- In the bottom middle is a visual of the TKE workstation and the optional devices it supports. More on TKE later.
- The Card Reader is the old 4754 and Personal Security Card from the TSS product family. These products are near end-of-life



- The Enablement Diskette is the method IBM uses to bypass/satisfy export controls and thus, be able to ship the Crypto hardware in all servers.
- Crypto Hardware is nonfunctional, 'brain-dead' without the data on the diskette
- Crypto module storage for keys and other crypto security data is nonvolatile, i.e., will not be affected by power loss to the server. This is due to the presence of a cryptographic battery unit, separate from the server battery, and providing up to 3000 hours of power. This battery is shipped 'powered off' to prevent power drain.



- The environmental setup is the information in the Options data set. The Options data set is pointed to in the ICSF Started procedure.
- The Options data set will in turn link back to the hardware crypto setup via the DOMAIN parameter.
- Also, in the Options data set are the names of the key data sets. Only the DES key data set, CKDS, is required.



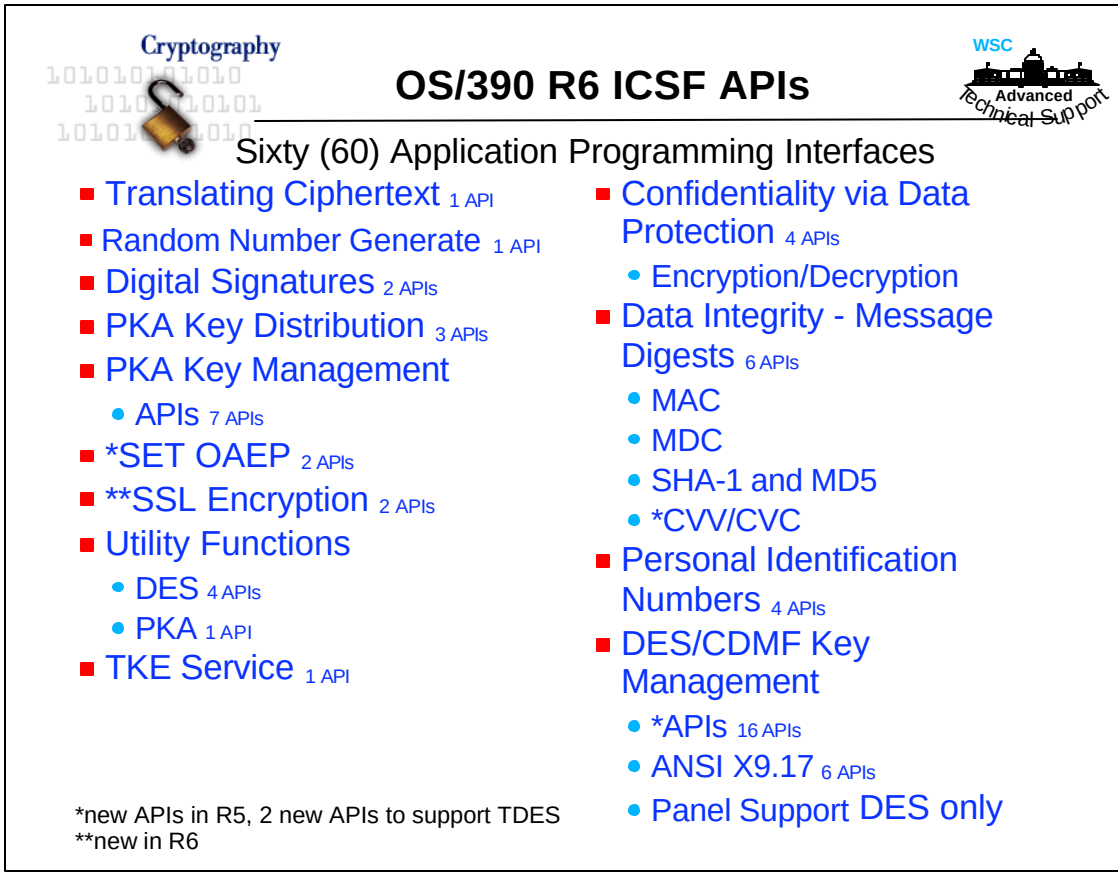
- This visual represents a system view of S/390 Crypto.
- The application code requesting crypto functions has been link-edited with the ICSF API stubs. Now, running in the user's address space, the stub code will cause a switch from the user's address space to the ICSF address space. ICSF will receive the request and
- query for access control requirements via SAF, System Authorization Facility, the front-end MVS process to RACF or ACF2, or other access control manager. It will check for the user's authority to any profiles protecting the name of the crypto key or the service.
- process any exits, if ICSF exits are present in the environment. There are ICSF exits for the initialization functions and environmental changes in ICSF as well as pre- and post- exit points for each API
- processes the API, verifying syntax and resolving the key token, if only the name of the key were passed in the API. The key token, in that case, will be obtained from the in-storage copy of the CKDS.
- ICSF now passes the request via machine instructions to the Crypto Coprocessor. Those machine instructions are not customer interfaces.
- The hardware takes the request and if a key token is passed in the request, the token is deciphered from under the protection of the Master Key associated with the Domain on which the application is running to obtain its value. The application key is then used to perform the requested task.

  If during this time the DES master key was changed, the application will not fail. This is due to a patented design by ICSF development. During the Master Key change the new key values are loaded into the AUX register which is known at that time as the New Master Key Register. When the key value is ready to become the real Master Key, the process requires the administrator to specify a new empty CKDS as input and the name of the current CKDS.

  Each record from the disk CKDS is read by the crypto hardware and the key values deciphered under the Master Key and re-enciphered under the New Master Key. Next, the administrator requests the master key to be changed. This causes the value in the NMK register to become the Master Key and the value that was the Master Key to become the Old Master Key, the AUX register now represents the Old Master Key Register. A copy of the newly re-enciphered CKDS is also read into a new ICSF data space. When any outstanding requests are complete, the data space containing the copy of the old CKDS is deleted.

  What happens to the application running is that the token retrieved from the in-storage CKDS will be sent to the Coprocessor and the hardware will check the MK verification pattern, a hash in the key token, to see if it matches the pattern of the current MK. If the MK verification pattern does not match, the pattern of the Old Master Key is checked. If it matches, the key is deciphered, the request processed, the key re-enciphered under the current Master Key. The results of the request, the new token along with a return code and reason code indicating the event will be passed back to the application.

- CAVEAT - all notes to this presentation are at a high-level and not all situations are explained in full or completely. There may be exceptions or special conditions required for the functional description to occur as explained.



- The older IBM Cryptographic Products
- PCF - Programmed Cryptographic Facility
- CUSP/3848 - Cryptographic Unit Support
- only provided 4 macros with which to perform cryptographic functions.

- ICSF as of OS/390 V2R5 (or with the January 1998 SPE on V2R4) provides a total of 58 unique callable services providing a wide range of function. In R6, R7, and R8 there are 60 APIs .

- The entire API set is described in the ICSF Application Programmer's Guide

- ICSF Customized and installation tasks are described in the ICSF System Programmer's Guide

- IBM offers an Installation Service for S/390 Crypto, ICSF, and TKE. There is also a 4.5 day class offered thru IBM Education and Training Services. The US code for this class is ES80A and outside the US the class code is ES800.

Supported Standards

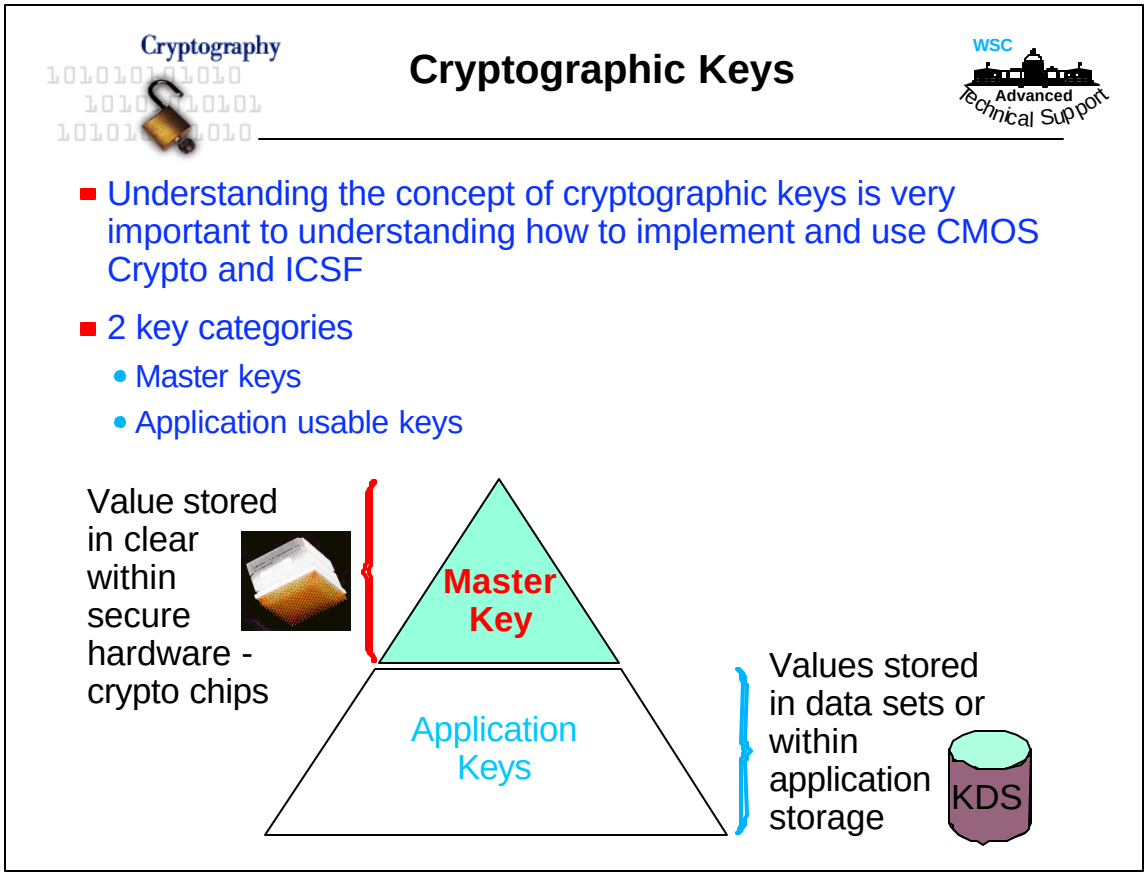
ISO 8730	BANKING - STD MES AUTH wholesale
ISO 8731	BANKING - APPR ALGOR FOR MESS AUTH (DES CBC with binary zero padding)
ISO 8732	INFO PROC - MODES OF OP - 64 BIT CIPHER ALGOR
ISO 8732 (1987)	BANKING - KEY MGMT wholesale
ISO DP 9564	PIN MGMT & SEC part 1
ISO 9796 (1991)	INFO TECH - SEC TECH - DIG SIG SCHEME GIVING MES REC (always with appendix)
ISO CD 10118 (7/92)	DATA CRYPT TECH - HASH OPS USING SYMM BLK CIPHR, ALGOR (MDC2, SHA-1)
ISO 10126	BANKING - PROC FOR MES ENCIPHER wholesale

Supported Standards . . .

■ FIPS 46-2 (1994)	Data Encryption Standard
■ FIPS 140-1 (1994)	Security Requirements for Cryptographic Modules
■ FIPS 180-1 (1994)	Secure Hash Standard
■ FIPS 186 (1994)	Digital Signature Standard
■ IETF RFC-1321	MD5 MESSAGING DIGEST STANDARD
■ ANSI X 3.92 (1981)	DEA
■ ANSI X 3.106 (1983)	MODES OF DEA OPERATIONS

Supported Standards . . .

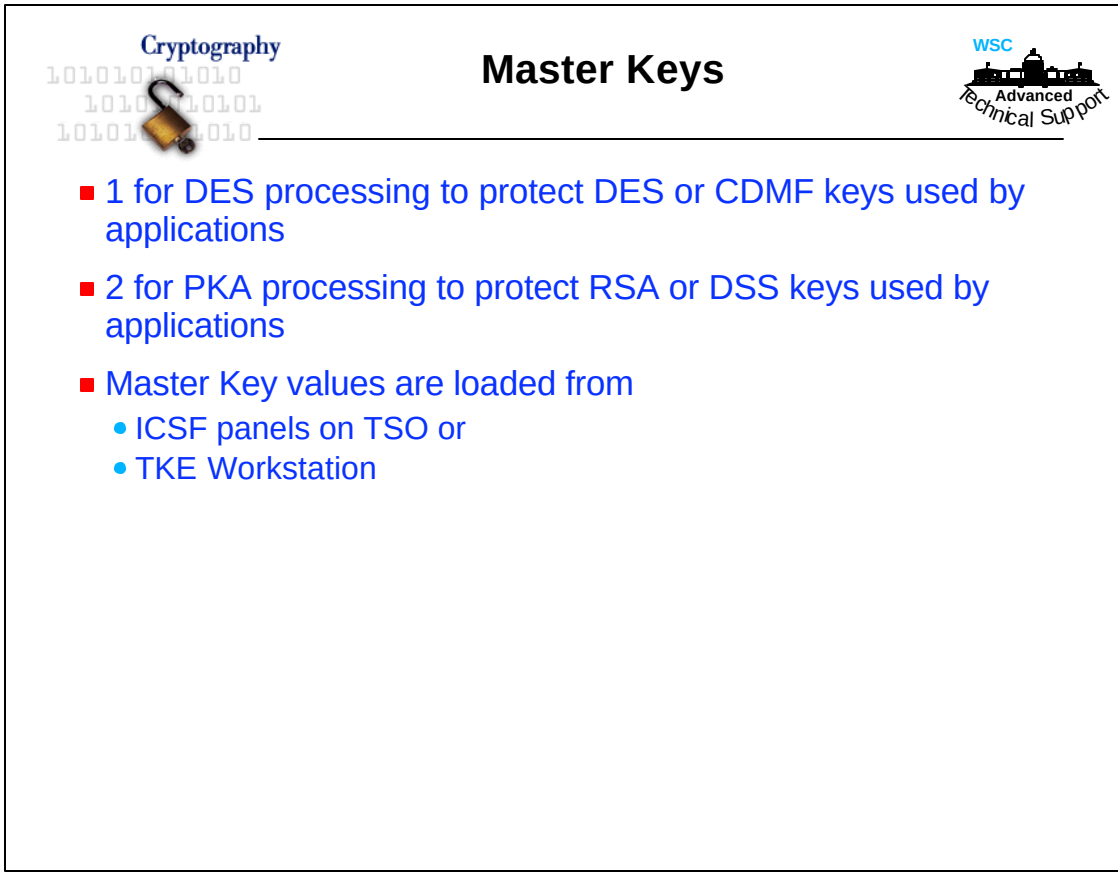
ANSI X 9.17 (1985)	BANKING - KEY MGMT 4753 in part
ANSI X 9.8 (1982)	PIN - MGMT & SEC
ANSI X 9.9 (1986)	BANKING - MES AUTH wholesale
ANSI X 9.23 (1988)	ENCRYPT OF WHOLESALE FINANCIAL MES
ANSI X12.42 (1990)	DRAFT - STD for Trial Use for Managining EDI Crypto SERV MES TRANS SET
ANSI X12.58 (1990)	DRAFT - STD for Trial Use for Managing EDI SEC STRUCT
ANSI X 9.52	TRIPLE DES FOR PRIVACY



- As you can see remembering what key is being acted upon or used is important. In the previous foil description of the Master Key change events it is the Master Key that is being changed. But, because it is used to encrypt the application key values stored in the CKDS, each of those is deciphered (or decrypted) and reenciphered to provide a valid token back to the application. Because the old master key is known any key enciphered under that value (as indicated by the master key verification pattern - MKVP) the value of the application key can be restored.

  It is this value that is used to perform the application's request.

- Many other things apply to the understanding of keys and are not discussed in this presentation. One of the most important is the concept of control vectors or variants.



- There is only 1 master key per LPAR to protect DES application keys. There is a DES auxiliary register that participates in the DES master key change process. It is known as the new/old master key register.

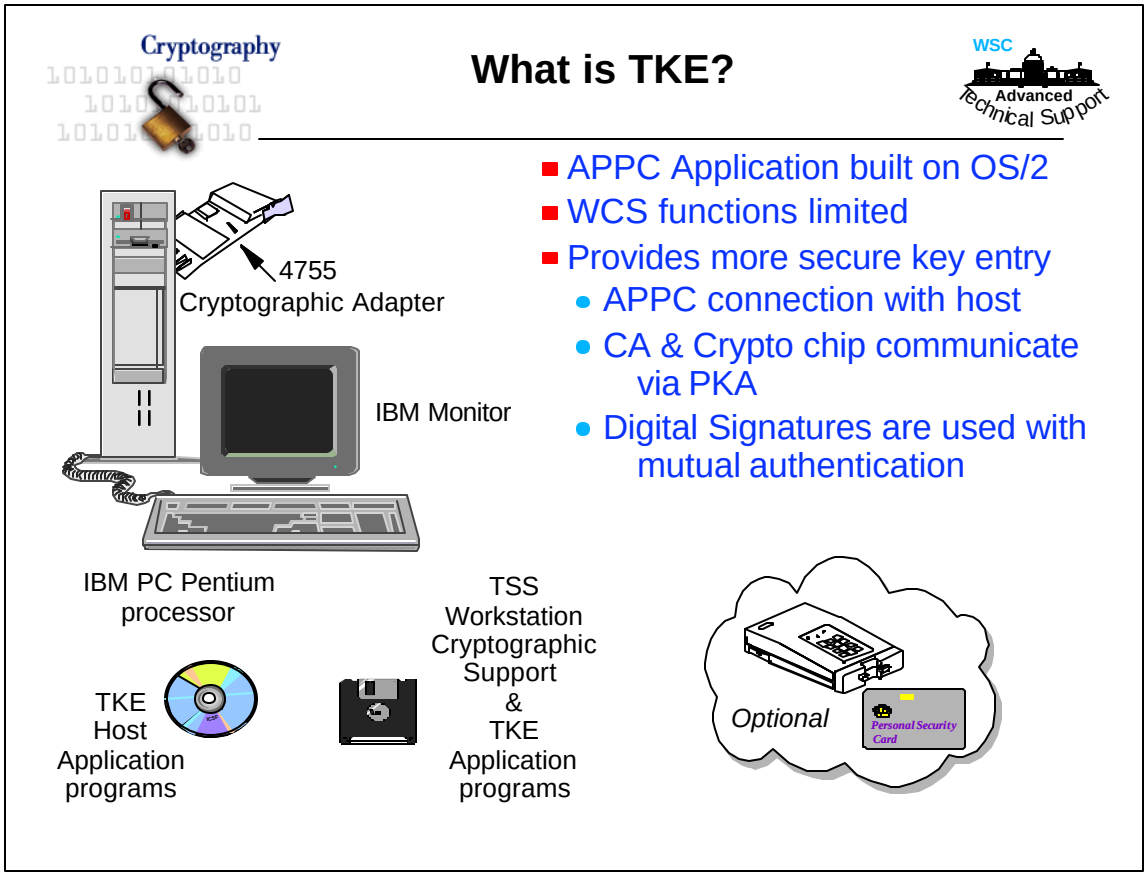
- There are 2 master keys per LPAR to protect RSA and DSS application keys. One of these protects application keys only used for digital signature processing. This master key is known as the Signature Master Key, SMK. The other protects application keys used for EITHER digital signature processing or the distribution of a symmetric key under a RSA public key. This is the Key Management Master Key or KMMK. (There were 2 master keys because of the export differences in key length between keys used for digital signatures and those used for key distribution. Export regulations have changed since that time and we now recommend that both the SMK and the KMMK have the same key value.)

- Master Key values can only be loaded via the ICSF panels or through the Trusted Key Entry Workstation, TKE.

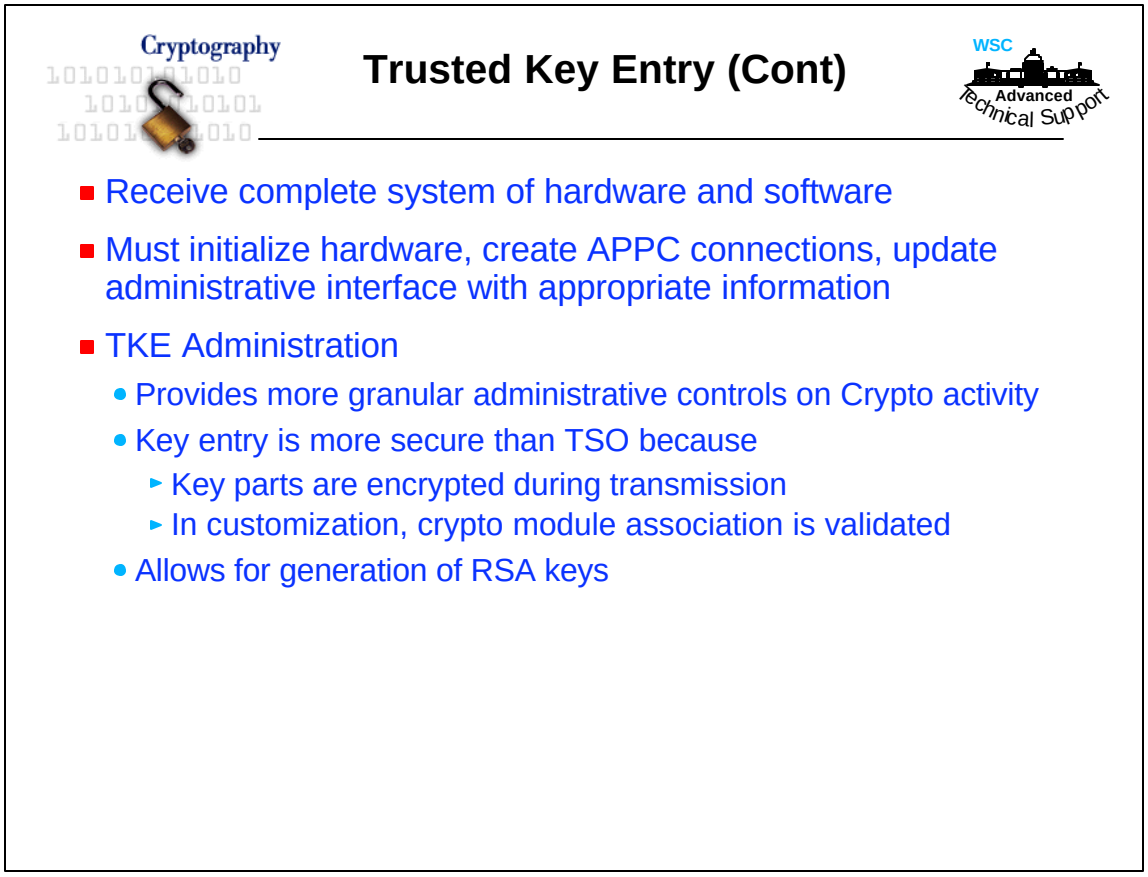
Application Keys

- Defined by either
  - Application via use of APIs
  - Administrator via ICSF utility
- 8, 16, or 24 bytes in length based on key type
- Placed in a structure for ICSF usage called a key token
- Key value is encrypted under the appropriate Master Key (DES, SMK, or KMMK)
- Can be stored within a record in a VSAM DASD key data set
  - CKDS is the DES/CDMF key data set
  - PKDS is the PKA key data set
- Keys can be given a label for easy reference by code

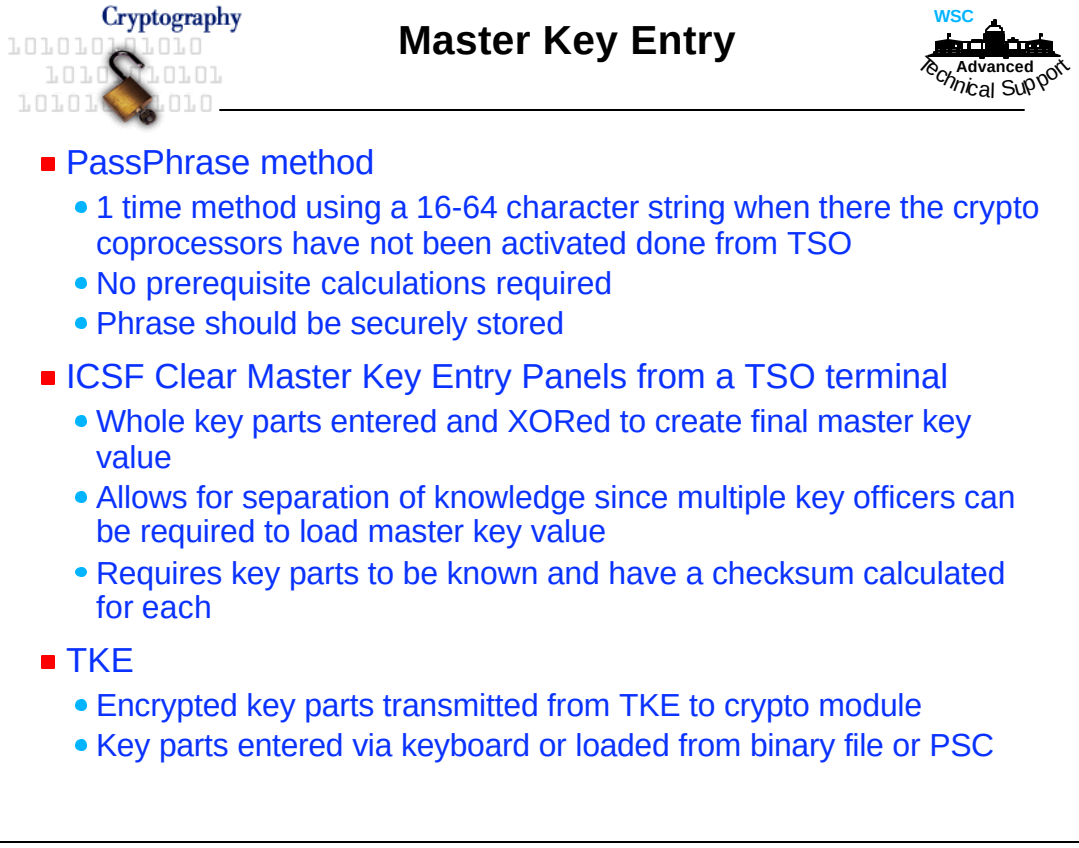
- Within the IBM CCA API set keys have associated with them
  - length,
  - type, and
  - form
- Application key values are the only encrypted data within a key token, other data in the key token is not.
- Key tokens that are in an internal form, having key values encrypted under the master key, are stored in the CKDS or PKDS, depending on the algorithm that produced the key. Keys produced using the DES algorithm are stored in the CKDS. Keys produced using a PKA algorithm (RSA or DSS) are stored in the PKDS.
- Control vectors are values that can be applied to the key PROTECTING a key to cause that key value being protected to be associated with a specific function. Other vendors, such as, Atalla, have a similar concept. They call theirs variants.
- To be able to exchange keys with other systems that do not recognize the IBM key structure or control vectors requires
- understanding that systems variants, if any
- encrypting the key value with a key that is known as a NOCV key. A NOCV key is a key that has been created such that no control vector will be applied to any key it is used to encrypt. Therefore, the encrypted key value has no additional data to be known by the receiver other than the value of the key supplying the protection. Keys protecting other keys in this fashion are called transport keys and have more explicit type names in ICSF API usage.



- The TKE Workstation is a complete hardware AND software solution
  - Hardware
    - PC with a 4755 Cryptographic Adapter card installed.
    - Monitor
    - Keyboard
  - Software
    - OS/2 system with Communications Manager/2 to provide the workstation APPC support
    - Emulator support so the administrator can have access to the MVS sessions and TSO
    - TKE application which uses some of the DKMS, Distributed Key Management System, product
    - Host software to support the host APPC requirements is included in OS/390
- TKE workstation security for Crypto depends on
  - the key values being encrypted by a Diffie-Hellman key during the transmission across the APPC connection to the host Crypto module
  - the TKE administrator having the ability to have unique signature keys associated with his ID number
  - the ability for the administrator to define granular security controls on the commands and functions provided by the TKE application
- When you order TKE, you are prompted to select the type of connection for the workstation: LAN Token-Ring or Ethernet. If you have a TKE and do not want another workstation, do not provide a selection and you will only get an Enablement Diskette indicating the use of a TKE but not the TKE workstation. No charge will be applied unless the connection is selected. (I believe)
- The Card Reader and Personal Security Card are optional features and have a charge associated with them. These devices are not documented in the ICSF or TKE manuals. They are documented in the Transaction Security System publications.



- TKE like the host Crypto must have some initialization performed for both hardware and software.
- The hardware initialization functions are
  - define master keys to be associated with the 4755 Cryptographic Adapter card
  - define transport keys to be associated with the 4754 and Personal Security Card (PSC), if these devices are to be used
  - provide protection of the cryptographic devices associated with the TKE
- The software initialization and customization functions are
  - setup APPC host and workstation connections
  - customize the TKE administrative interface based on policy



- Master Key entry of the DES Master Key MUST be done before the S/390 Crypto environment is usable by applications
- The 3 methods for Master Key entry are listed
- ICSF Clear key entry from Panels implies a TSO session the key values loaded via this method are exposed during the transmission to the crypto module. Each site must determine the risk associated with this.
- Master Keys are loaded in parts. Each part is a complete length of the master key value. DES Master Key must be loaded using at least 2 parts, more parts could be used. PKA Master Keys, SMK and KMMK, can be loaded using a single part. The recommendation is for the SMK and KMMK to have the same value.
- SMK and KMMK are 2 unique master keys in order to support the export requirements. SMK allows key lengths of up to 1024-bit for both US/Canada and non-US/Canada customers. KMMK, for symmetric key distribution, allows a selection of key length based on export restrictions associated with the customer. US/Canada customers can have PKA public keys for key distribution with key lengths of 1024-bit. Non-US/Canada customers are limited to 512-bit length keys.

S/390 Crypto Exploitation

- BSAFE - RSA Data Systems
  - Version 3 special code
  - Algorithm Methods for limited subsets of ICSF APIs
- Communication Server/2 allows LU 6.2 SLE
- Access Method Services - REPRO command
  - PCF macro calls, requires ICSF in COMPAT mode
- OS/390 Domino.Go Web Server
- WebSphere HTTP Server
- OS/390 Firewall Technologies
- OS/390 eCommunications Server - IPSec
- OS/390 TN3270e

S/390 Crypto Exploitation (Cont)

- DCE Security Server - RPC
- VTAM
  - Session Level Encryption - V3R4.1 - Encryption
  - Message Authentication - V4R4 - MAC
- S/390 Payment Gateway Server
- RACF OS/390 Security Server R5
  - Can specify storage of cryptographic keys within ICSF disk data sets.

Note: This is not a complete list of exploiters.