



IBM Americas, ATS, Washington Systems Center

Crypto and the Trusted Key Entry Workstation: Is a TKE In Your Future

Share 12686

San Francisco, CA February, 2013

Greg Boyd (boydg@us.ibm.com)

IBM Americas ATS, Washington Systems Center

© 2013 IBM Corporation



QR Code

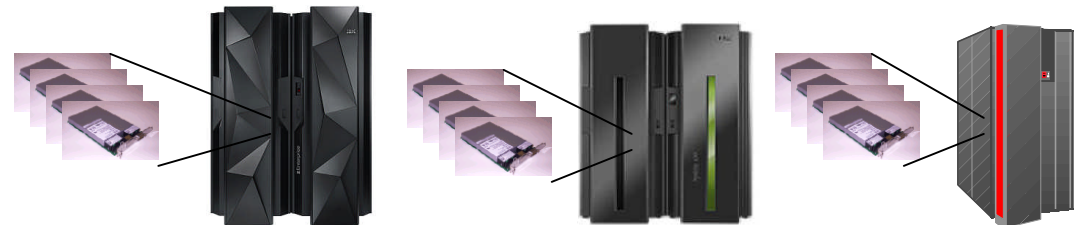


Agenda – TKE In Your Future

- **What is it? What does it do?**
- **How It Works**
- **Some Terminology**
- **Smart Cards**
- **TKE History**
- **TKE Exclusives**

TKE – What does it do?

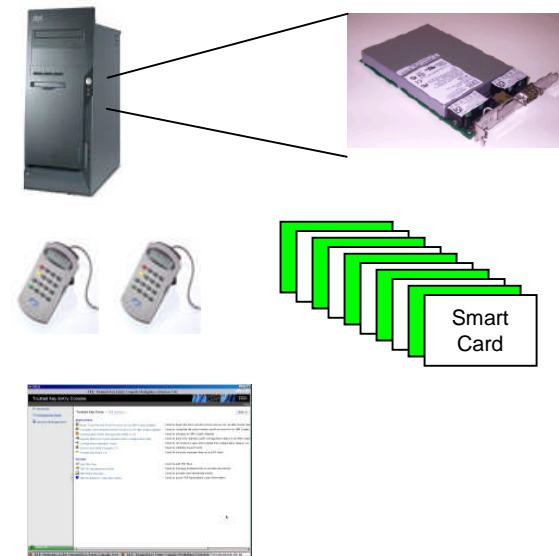
- **Provides secure key entry**
 - Key material is generated in hardware and never exists in the clear outside of the tamper hardware (security)
 - Can provide dual control (integrity)
- **Provides utilities for configuration management of the host crypto**
- **It doesn't do**
 - Crypto for applications
 - Key storage



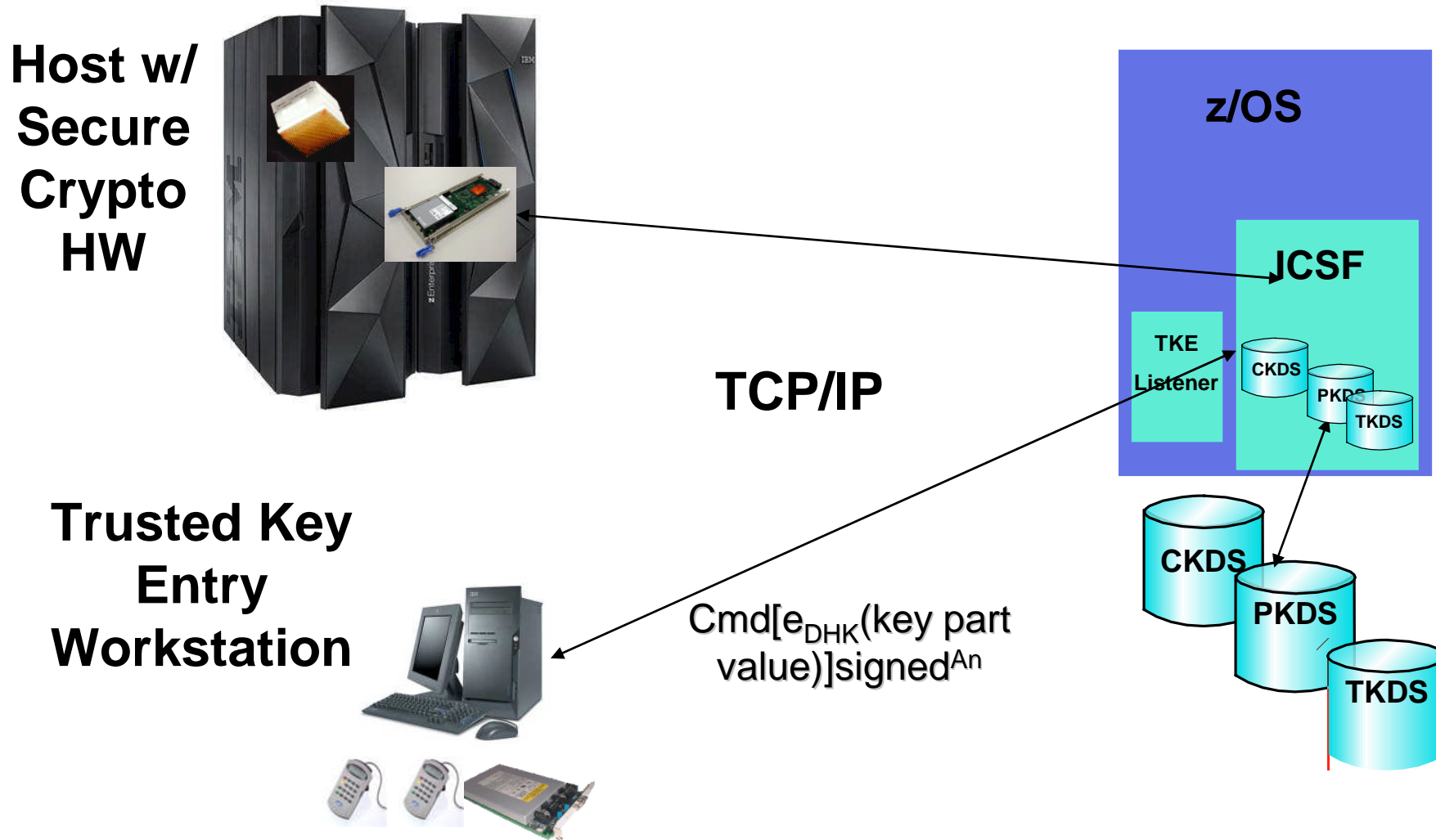
TKE – What is it?

TKE workstation with a Crypto Coprocessor

- Intel Workstation (FC 0841) with an embedded operating system
- Cryptographic coprocessor
- Optional TKE smart card support
 - Readers and 20 smart cards (FC 0885)
 - 10 Additional smart cards (FC 0884)
- A TKE application (Java) (FC 0850)



TKE – Trusted Key Entry Workstation



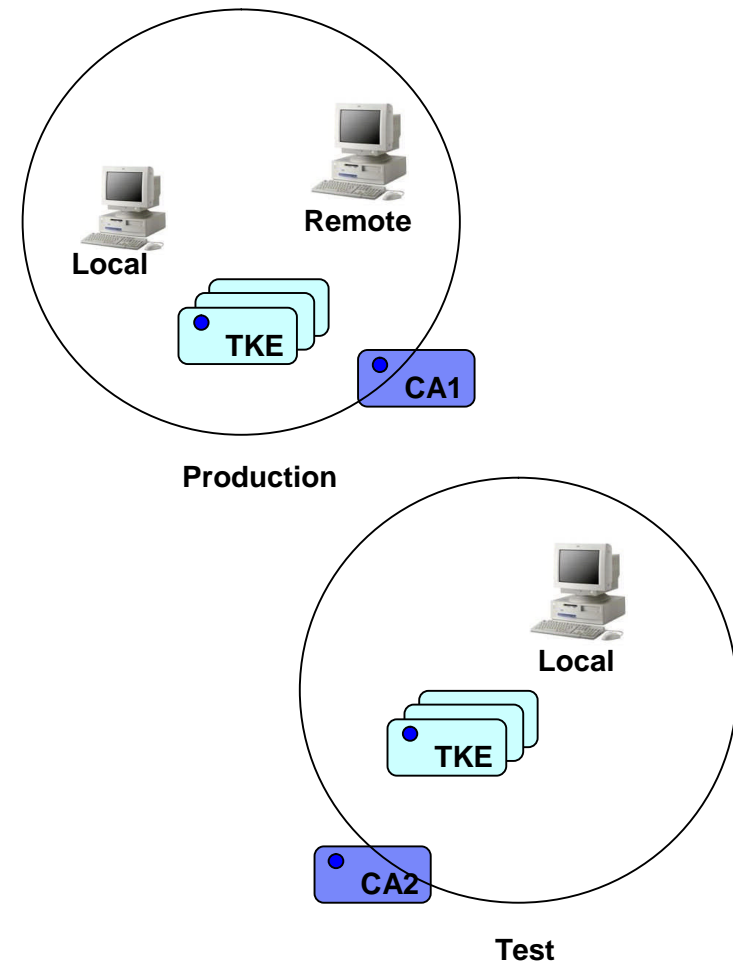
TKE Zone

A TKE zone is a set of Smart Cards and TKE local Crypto Adapters that share a common CA (Certificate Authority) Smart card.

A security concept ensuring that only members of the same zone can exchange key parts. It is established by a CA smart card, and is made up of entities:

- **CA Smart Card**
- **TKE Smart Card**
- **TKE Cryptographic Adapter**

Key material can ONLY be passed between Smart Cards or Smart Cards and the TKE's local crypto adapter, when the Smart Cards and/or TKE local crypto adapter are in the same TKE zone.



Security across the connections

- **TKE Workstation Crypto Adapter**

- Profiles
- Roles

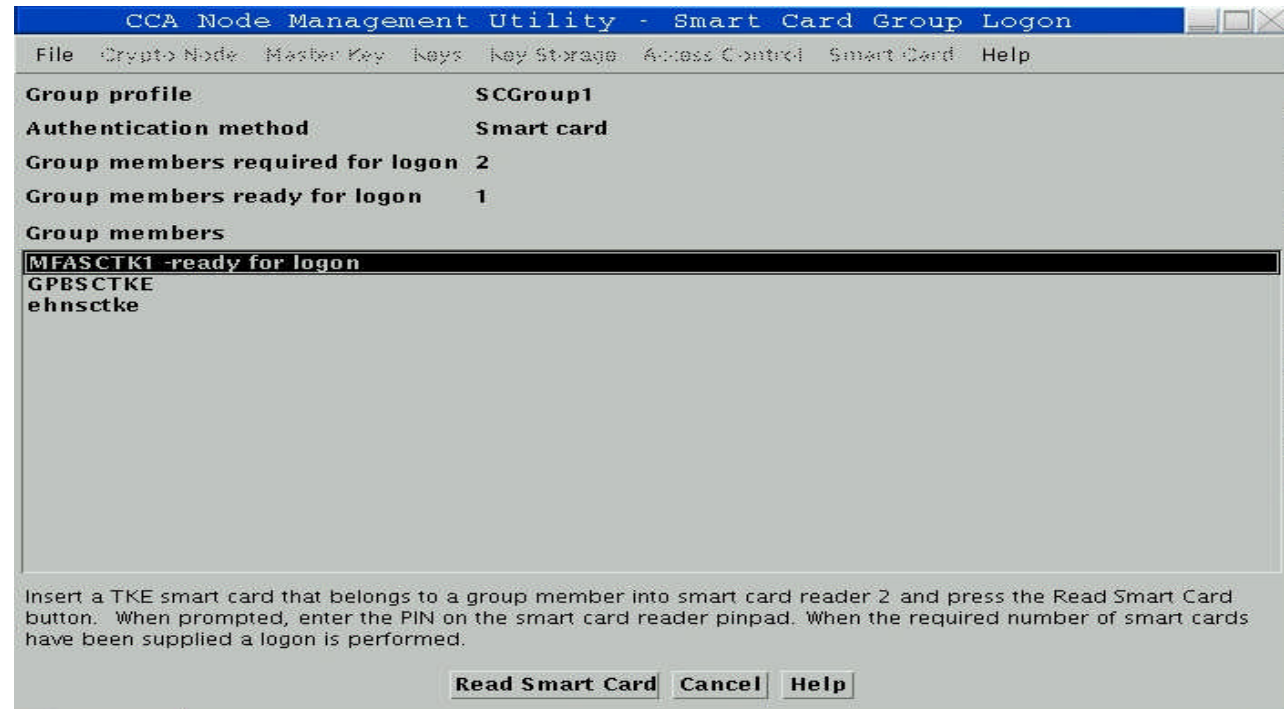
- **Host Crypto Adapter**

- User/Authority
- Roles

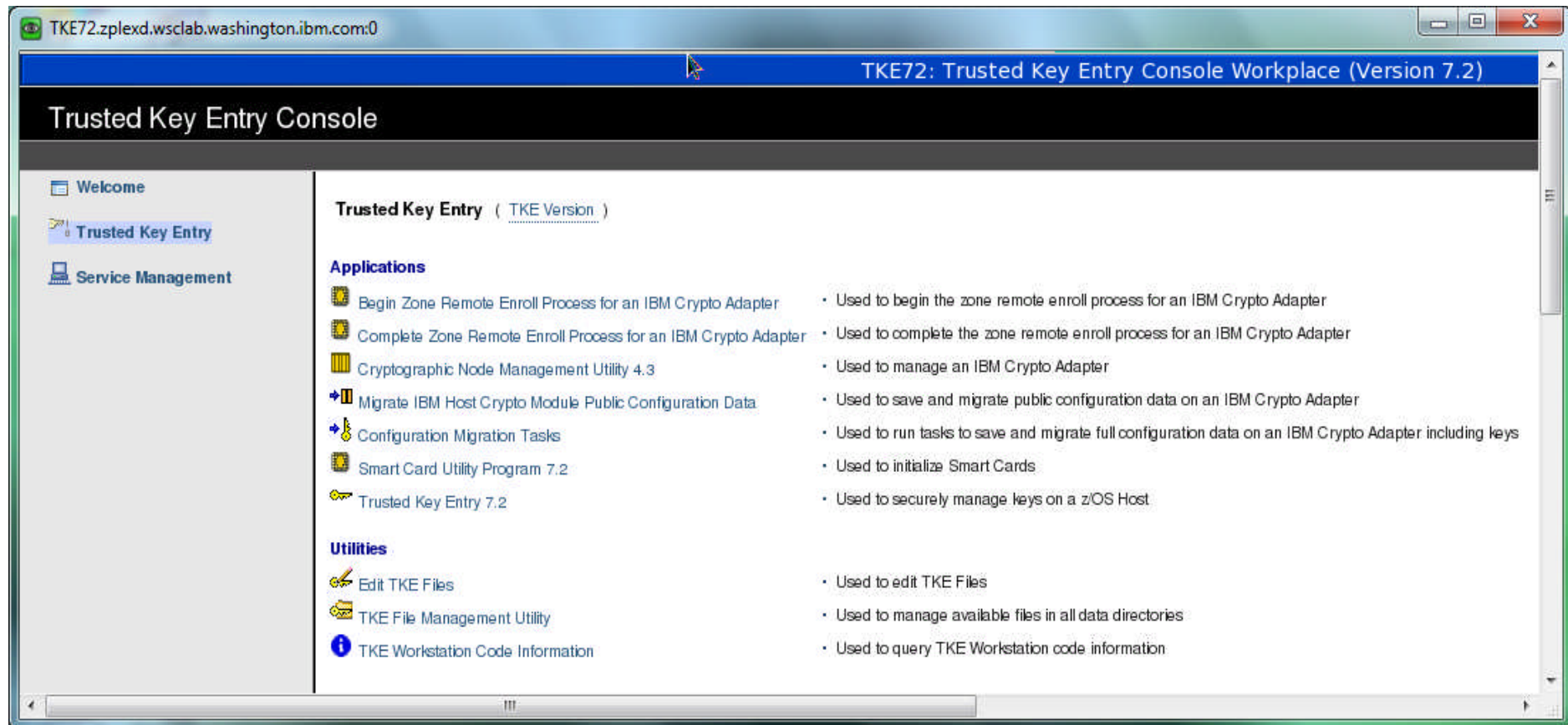


Group logon feature

- Enables dual and multiple control of workstation commands by requiring a certain number of users to authenticate to the TKE as members of a group.



TKE Main Menu

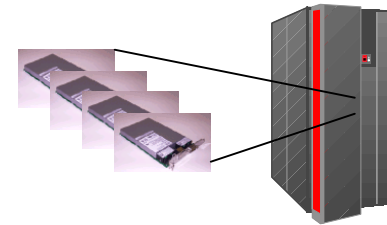


Management of Host Adapters:

Load master keys (Also supports loading of many operational keys)

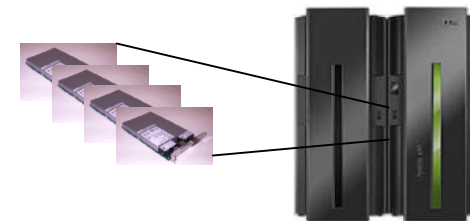
- Dual controls
- Hardware bases *
- Optional smart cards * – key material never in the clear outside a crypto engine

* Required by laws, regulations and/or standards



Migration of Host Adapter information from one adapter to another

- Public information
- Card cloning
- Cross LPAR/Cross CEC
- Information moved to equal or newer adapter

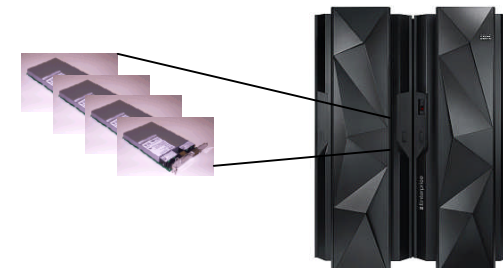


Host adapter has 16 domains (each with set of master keys)

- TKE allows domains to be grouped and managed as 1

Manage access to adapter services

- What crypto services can be used
- What pin decimalization tables can be used
- Some default adapter settings



TKE Groups

Trusted Key Entry

Function Utilities Preferences Help

Hosts

Host ID	Description
Billh	
cp	
hz	
s0C	
s21	

Crypto Module Groups

Group ID	Description

Domain Groups

Group ID	Description
break	
dg1	
SetDEC	

Crypto Modules

Host ID	CM index	Status	Description

Help

Signature Key Loaded, Index: 0, Name: Default

Crypto Module Notebook

The screenshot shows the 'Crypto Module Administration' window for 'Crypto Module : cp / G35'. The 'Domains' tab is active, displaying a table of 'Domain Keys'. Below the table, a 'Select key to work with' dropdown menu is open, showing a context menu with options like 'Generate single key part...', 'Load all key parts from...', and 'Smart card'. Red boxes and numbers 1 and 2 highlight specific elements in the interface.

	Status	Hash pattern
New AES Master Key	Empty	0000000000000000
Old AES Master Key	Valid	BF494FF74B86343F
AES Master Key	Valid	2058C870E9D3194F
New ECC Master Key	Empty	0000000000000000
Old ECC Master Key	Empty	0000000000000000
ECC Master Key	Invalid	0000000000000000
New DES Master Key	Empty	00
Old DES Master Key	Valid	2B0C723D1AB9C948E9C9E32E7FF3B7F4
DES Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
New Asymmetric Master Key	Empty	000
Old Asymmetric Master Key	Valid	EF4C65754B5088C22D03480BC7B952B2
Asymmetric Master Key	Valid	E83F158521FEEA23986CC9483DAFD711

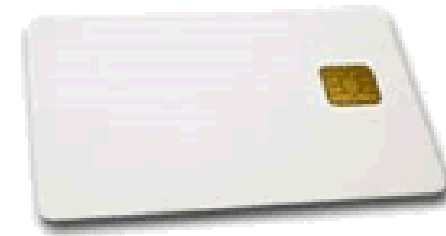
Key Type: Master Key - AES:
AES Master Key
ECC M
Master k
DFS M

Context Menu Options:
Generate single key part...
Generate multiple key parts to...
Load single key part
Load all key parts from... (1)
Clear
Secure key part entry
Smart card (2)
Binary file
Keyboard

Smart Card part 74Y0551

- Smart cards used to:
 - Hold credentials
 - Hold key material
 - Perform encryption functions.

Smart Card Support – TKE Zones



- **Certificate Authority (CA) Smart Card – Establishes the zone (two, 6 digit PINs)**
- **TKE Smart Card – Used for storing keys & key parts (6 digit PIN)**
 - Generates, stores and uses a TKE crypto adapter logon key
 - Store Key Parts
 - ICSF (host) key parts, both master and operational keys
 - Optionally, store TKE crypto adapter workstation master key parts
 - Generates, stores and uses a TKE authority signature key
- **EP11 Smart Card – Required for loading P11-MK and storing keys & key parts**

Smart Card Support - Configuration Migration

- MCA (Migration Certificate Authority) - for defining zones associated with the migration wizard
- Key Part Holder – for holding parts of a master key being transported
- Injection Authority – for injecting master keys into new adapters

TKE Version History

■ TKE 5.3 (2008)

- Auditing – Added security relevant event Audit Log with hundreds of auditable events
- AES support
- USB readers and new smart card

■ TKE 6.0 (2009)

- Domain Grouping
 - Domain scoped operations (e.g. key loads) are broadcast to all domains in the group in a single operation
 - Adapter scoped operations (e.g. create authority) are broadcast to each adapter in the group in a single operation
- Migration Wizard – capture configuration data from the adapters on the host and push that to another card

■ TKE 7.0 (2010)

- Full-function host cryptographic adapter migration wizard includes capturing key material

TKE Version History (cont.)

■ TKE 7.1 (2011)

- New wizard for loading/generating keys
- New ACPs for TKE applications
- Migrate roles utility
- New AES operational keys
- PIN Decimalization Table support
- Host cryptographic module status
- Support for up to 50 key parts
- Display active ids on the TKE console
- Use of Elliptic Curve Diffie-Hellman (ECDH)
- Enhancements to full-function migration wizard

TKE Version History (cont.)

- **TKE 7.2 (2012)**

- EP11 (IBM Enterprise PKCS #11) support
- Support CEX4SC
- New DES operational keys (associated with CipherTextTranslate API)
- New AES Cipher key attributes
- Allow creation of corresponding keys
- Support up to 4 smart card readers

TKE Exclusives

- **Secure loading of master keys**
- **Migration Wizard**
- **Loading MKs for inactive LPARs**
- **Enabling/Disabling ACPs**
 - 24-Byte DES-MK
- **Loading PIN Decimalization Tables**
- **Loading P11-MK**

Questions ...

IBM Advanced Technical Support – Washington Systems Center



Time for...



QR Code

