Understanding the Crypto Hardware Available for zSeries and S/390

As of December 2001 there are 3 types of cryptographic hardware available for use with IBM zSeries processors: the standard Cryptographic Coprocessor Facility (CCF), and the optional charged adjunct features: PCI Cryptographic Coprocessor (PCICC) and PCI Cryptographic Accelerator (PCICA). PCI is the acronym for Peripheral Component Interconnect. For S/390 CMOS processors there are only 2 types of cryptographic hardware available: the standard Cryptographic Coprocessor Facility (CCF) and the optional, charged the adjunct PCI Cryptographic Coprocessor (PCICC) feature.

All cryptographic hardware features can be shared across LPARs. Cryptographic hardware is not available on coupling facility models. The adjunct features require the presence of an enabled CMOS Cryptographic Coprocessor Facility (CCF).

The 3 crypto hardware features are accessible in z/OS and OS/390 only through use of the Integrated Cryptographic Services Facility (ICSF) software, a component of the OS/390 and z/OS base in the Cryptographic Services element. ICSF is used to load system Master Keys into the hardware allowing it to process cryptographic functions. ICSF is also the means by which applications request cryptographic services by using the appropriate Application Programming Interfaces (APIs) or service calls. ICSF communicates with the crypto hardware via machine instructions that are not Programming Interfaces nor publicly documented.

The cryptographic hardware features are completely managed by OS/390 or z/OS Integrated Cryptographic Services Facility, with cryptographic requests balanced across all available crypto engines that can handle the specific function. Some functions are only available on a specific type of coprocessor and not on the others. Some functions may be routed to a specific type of coprocessor even though other types can also process that function. The decision process is made by ICSF. For those functions requiring a specific type of coprocessor the ICSF API will document the specific requirement.

This paper provides an overview description of each crypto hardware feature and summary tables on how each differs from the other crypto hardware and what each requires for use by applications. The Trusted Key Entry Workstation will be briefly described. Also, the crypto Linux support will be briefly described. This paper contains the following sections:

- Description
- Reference Tables for Features Differences, Capabilities and Requirements
- Summary of Crypto Hardware Ordering Overview

Technical Documents related to mainframe cryptography will be placed on the ATS TechDocs web site http://www-1.ibm.com/support/techdocs/atsmastr.nsf. Use SEARCH ALL DOCUMENTS and keyword, CRYPTO, to locate documents.

Data herein has not been formally reviewed by IBM. Attempts are made to kept information as current as possible, however, you should check for the most recently updated copy on the ATS TechDocs web site.

Trademarks are noted at the end of this document.

Description:

Cryptographic Coprocessor Facility (CCF)

This is the standard installed cryptographic hardware available on most IBM CMOS and zSeries processors today. There can be no more than 2 CCFs per server (machine). The number of actual CCFs available for use vary based on model and configuration of the server. For more details see the technical document "Reference for Number of Crypto Coprocessor Available to a Server by Model" on the web site http://www-1.ibm.com/support/techdocs/atsmastr.nsf using SEARCH ALL DOCUMENTS and keyword, CRYPTO. Any charges for the CCFs are generally associated with the enablement diskette.

The cryptographic hardware is shipped nonfunctional. CCFs are made functional by the loading of crypto configuration data from an enablement diskette. The enablement diskette contains information regarding the type of algorithms and key lengths the installation is allowed to use in its cryptographic operations. The single diskette will contain configuration data for both crypto modules available on the server if more than one is available.

This diskette is created with dependencies to the specific server and the cryptographic modules installed within that server to meet export regulation restrictions. Diskettes should be managed to prevent erasure or loss since replacements may take up to two weeks to obtain. A new diskette is provided whenever a hardware change requires the replacement of one or more crypto modules or a different crypto configuration has been ordered for a server. This diskette is the property and responsibility of the customer.

The IBM CE loads the files for each crypto module from the diskette into the server's Support Element where it resides until it can be copied into the physical module. The actual loading of the data into the cryptographic module occurs as a result of a Power On Reset based on the selection options chosen for next activation by the CE. Thus, enabling the CCF is a disruptive process. The enabling may need to occur again if

- a tamper is detected or CCFs are replaced due to processor upgrade, or
- the CCFs are zeroized from the Cryptographic Coprocessor Configuration task, or
- the configuration data is erased from the support element by a system operator, or
- a MCM board replacement occurs.

Diskette configuration activation causes the clearing of all system master keys and all other secure cryptographic data stored within the affected modules. System Key Officers, those responsible for loading the system master key parts, must be notified prior to this operation to ensure as little impact to production cryptographic operations as necessary.

The cryptographic hardware is designed to perform a specific set of functions that were architected into the physical chip. These functions are stabilized in the CCF and all new functions will be provided in the adjunct PCICC feature. Cryptographic Coprocessor Facility supports the following algorithms for application use based on configuration order: Triple-DES, DES, CDMF (40-bit), RSA for key management and digital signature and DSS for digital signature. For specific information concerning algorithms or standards consult the ICSF Application Programmer's Guide.

The CCF is physically attached to a CP (central processor) and thus, access to the available crypto coprocessor engine may be limited based upon workload requirements to the CP to which it is attached. Also, availability to a CCF may be at risk, depending on the server model, on loss of the CP or even loss of a CCF. Crypto availability was enhanced with the introduction of the "twin-tail" attachment for the CCFs. Starting with G5, the physical attachment of each cryptographic module is made to two (2) CPs. Only one physical connection is active at any time to a crypto module. At the loss of the primary CP path, access to the CCF is provided via the second connection during recovery processes.

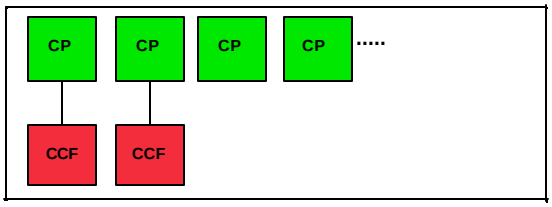

Figure 1. CCF attachment to CPs prior to G5.

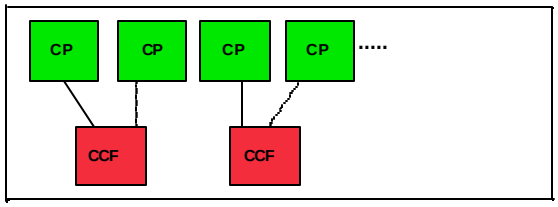

Figure 2. CCF attachment to CPs in G5 & higher.

The CCF features are accessible in MVS, OS/390, and z/OS environments only.

PCI Cryptographic Coprocessors (PCICC)

Available beginning June 30, 2000, this additional cryptographic hardware is orderable on IBM G5, G6 CMOS, and zSeries servers. PCICC is an adjunct coprocessor because it requires the presence of a CCF and extends the scalability of crypto processing. There can be no more than 8 adjunct crypto features per server.

Each PCICC feature is built around an IBM 4758-2 PCI Cryptographic Coprocessor card embedded in an adapter package for installing within a G5 or G6 server. For CMOS G5 and G6 servers a PCICC feature will contain a single PCICC card. PCICC features ordered for zSeries servers will contain dual (2) cards. The table below displays the relationship between features and the maximum number of cryptographic engines available for each server type. Note that the total number of all adjunct engines on a server may not exceed 8.

	Feature Code	Maximum Features	Maximum # of Crypto Engines
G5 and G6	0860	8	8
zSeries	0861	8	16

The adjunct cryptographic feature, PCICC, comes in **separate packaging** and needs to be re-plugged prior to power on. The PCICC is shipped in separate packaging whether the order was generated as a MES or part of a new processor order. The separate packaging is due to temperate controls that must be maintained to prevent damage to the hardware, FC0861. There should also be a FCV diskette shipped. This diskette contains the configuration data to be associated with all PCICCs installed on that particular processor. As with the Cryptographic Coprocessor configuration diskette, the PCICC diskette is the property of the client.

It is important to remember this separate packaging is sent to ensure that the hardware installation is performed during the maintenance window assigned.

The cryptographic hardware is shipped nonfunctional and is made functional by the loading of microcoded crypto Function Control Vector (FCV), also known as the PCICC enablement diskette. The PCICC enablement diskette contains information regarding the type of algorithms and key lengths the installation is allowed to use in cryptographic operations. This diskette must match the configuration selection used in the CCF(s) on the server. The CCF configuration must be loaded prior to the FCV loading in servers running OS/390 or z/OS.

Unlike the CCF enablement, the enablement of the PCICC cards is nondisruptive. The FCV configuration is stored in the HSA (Hardware System Area) and therefore, available to each PCICC as they are defined as being active and online to the system(s). The FCV is then copied from the HSA to the PCICC cryptographic card module. Thus, each card shares the same configuration file and the file need only be loaded into HSA where the configuration is immediately available to each PCICC as they are made active.

The PCICC hardware is designed to perform those functions supported by the CCF plus newer functions that correspond to functionality that was available in the withdrawn, 4753 Cryptographic product. The newer functions include encrypted PIN processing, RSA key generate, and new key management functions. These new functions enable migration of applications written for the withdrawn IBM 4753 Transaction Security System, a channel attached crypto unit. ICSF will transparently route application requests for cryptographic services. Either a CMOS Cryptographic Coprocessor or a PCICC will be invoked (depending on performance cryptographic function) to perform the cryptographic operation.

PCICC programmability supports the ability for rapid implementation of new cryptographic standards.

Customized crypto functions needed in unique customer situations can be supported through the User Defined Extension (UDX) capability of PCICC and z/OS. Customers will work with IBM for implementation services, testing, and digital "signing" by IBM to ensure proper UDX operation. The programmability of PCICC's make these features very flexible to customer requirements and solutions. The PCICC feature supports public key sizes up to 2048 bits.

The PCICC is not physically attached to any CP (central processor). The packaging of the PCI crypto feature provides attachment through the Self Timed Interface. It has an I/O Bus and requires CHPID association but does not require IOCP definition.

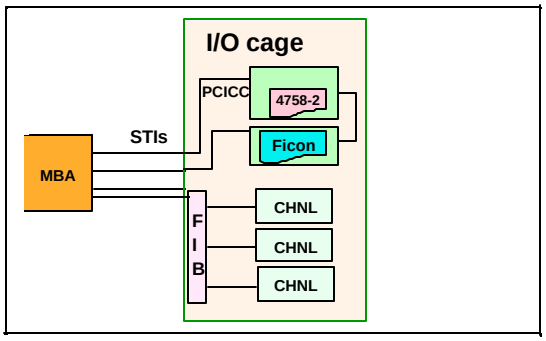

Figure 3. PCI feature STI attachment to the Memory Bus Adapter inside the CEC cage.

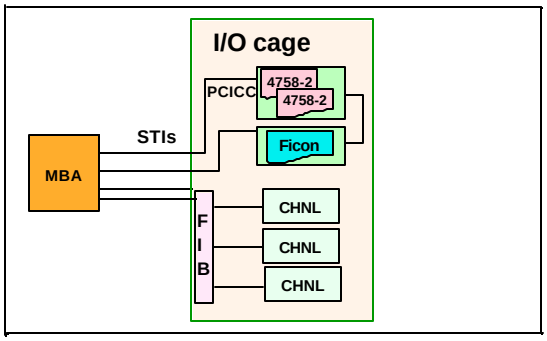

Figure 4. PCI feature STI attachment in zSeries to the MBA inside the CEC cage.

The PCICC feature is applicable to both OS/390 or z/OS and Linux environments on IBM G5/G6 and zSeries servers. In zSeries Linux environments if a PCICA feature is also enabled, the PCICC feature is ignored due to the faster SSL crypto processing on the PCICA. Since only the clear key application programming functions are provided for use in the Linux environment and the PCICA feature was designed for just those functions, PCICA offers much greater SSL throughput than the PCICC. The speed at which the PCICA can handle the clear key requests makes the PCICC an unnecessary crypto device in the Linux environment.

PCI Cryptographic Accelerator (PCICA)

New in 2001, the PCICA is a new cryptographic coprocessor available **only** on **zSeries** servers and requiring z/OS V1R2. This new addition to the mainframe cryptographic hardware is only available on IBM zSeries processors. The feature code for the PCICA is 0862. There can be no more than 6 PCICA crypto features per server. PCICA is another adjunct crypto coprocessor designed specifically for exploitation by SSL. This crypto coprocessor was designed to extend the scalability of SSL transactions. Note that the total number of adjunct coprocessors possible on a server cannot exceed 8 of any combination of PCICC and PCICA features.

	Feature Code	Maximum Features	Maximum # of Crypto Engines
zSeries	0862	6	12

The adjunct cryptographic feature, PCICA, comes in **separate packaging** and needs to be re-plugged prior to power on. The PCICA is shipped in separate packaging whether the order was generated as a MES or part of a new processor order. The separate packaging is due to temperate controls that must be maintained to prevent damage to the hardware. It is important to remember this separate packaging is sent to ensure that the hardware installation is performed during the maintenance window assigned.

Each zSeries PCI Cryptographic Accelerator Feature contains two crypto cards. In testing, a single dual card feature supported up to 2100 SSL handshakes/sec. However, the maximum number of SSL handshakes/sec that can be supported on a zSeries server by any combination of CMOS crypto, PCICC crypto, and PCICA crypto is limited by the amount of CPU cycles available to perform the software portion of the SSL handshake. Two features (4 cards) is currently enough to drive the maximum rate of 3850 SSL handshakes/second announced in the October 4, 2001 hardware announcement 101-308.

This feature should be used where maintaining high numbers of SSL handshakes per second is required for service agreements associated with web applications. Having one or more of the PCICA features in addition to the CCF(s) and one or more PCICC(s) will ensure throughput for SSL-based transactions can be maintained at very high numbers while other non-SSL crypto workloads are also processed. Applications that call ICSF directly for "clear key" RSA operations, will also transparently use the zSeries PCI Cryptographic Accelerator Feature. The PCICA feature supports all public key sizes up to 2048 bits.

To use PCICA, the zSeries processor must be at Driver 3CG. There is no configuration data to be loaded for the PCICA feature enablement. LPAR association via specification of the candidate's list is required just like PCICC definition. There is only one page in the image profile for association of the adjunct coprocessors to a logical partition. The tab for that page is labeled PCI Crypto.

The PCICA cryptographic hardware feature is designed to perform a very limited set of functions to support SSL cryptographic functions. No data privacy, financial, or key management operations are included in the PCICA design. Therefore, no tamper requirements or battery backup exist for the PCICA cards.

The PCICA is not physically attached to a CP (central processor). This feature is a Self Timed Interface card. It has an I/O Bus and requires association with 2 CHPIDs but does not require IOCP definition. See Figure 4 on the PCI feature attachment under PCICC description.

The PCICA feature is only applicable to zSeries servers.

Trusted Key Entry Workstation

The TKE is a combination of hardware and software supporting the TKE application system. The TKE workstation is network-connected to System/390 and zSeries hardware and software. Trusted Key Entry (TKE) is an optional feature of ICSF that provides a basic key management system. It is a tool for security administrators to use in setting up and establishing the security policy and placing it into production.

Physical protection of the TKE Workstation will be required. The TKE application is OS/2-based. The workstation is delivered complete with crypto hardware and all software required to support the application. Initialization of the workstation cryptographic hardware, connectivity setup to the host systems, and any customer desired administrative customization is required. The TKE will have an emulator available for host ICSF access. This workstation is considered a part of the server system for any maintenance and support issues. No other application code should be added to the TKE workstation.

TKE is not the key storage vehicle nor does it perform the cryptographic functions requested by OS/390 and z/OS applications using the ICSF APIs. TKE is strictly a more secure way of entering key values into the cryptographic environment rather than using the ICSF TSO panels provided with the base ICSF support. However, all key entry must be completed using the ICSF panels to move the key values from the secure hardware temporary areas to the final storage locations. With a TKE workstation multiple machines and LPARs can be managed remotely.

TKE key entry allows for the entry of all but DATA keys for privacy or CVC/CVV processing to be entered as "parts". Key parts are strings of hexadecimal digits the complete length of a key that when XOR'ed together create the true, final key value. This eliminates the need for any single individual to have access to a complete, true key value. These key parts flow across the connection encrypted under a 24-byte Diffie-Hellman derived symmetric key. TKE also provides mechanisms

for a tight granular control of functions that can be performed related to key management, crypto module, domain management, and the management of authorities assigned to use the TKE application.

Order TKE if

- having a key part appear in the clear outside of the hardware is an not acceptable risk,
- having key part entry be a tightly auditable controlled event is a requirement,
- managing multiple servers and LPARs is required from a single location or key administrators are at remote locations.

Sample code for entering

- DATA key in parts from TKE and
- entering key parts from ICSF panels

is available from the ATS Techdocs web site http://www-1.ibm.com/support/techdocs/atsmastr.nsf. Use SEARCH ALL DOCUMENTS and keyword, CRYPTO, to locate the sample applications.

Function	TKE	ICSF Clear Panels	Sample ATS Code
System Master Key entry by key parts (dual custody)	x	x	-
DES application key entry by key parts (dual custody)	x	-	for both TKE & panels
Granular control over key entry	x	-	-
Capability to zero crypto info for a single LPAR	x	-	-
Capability to reduce Master Key entry effort	x	new in z/os 1.3	-

Crypto Support for Linux

The PCICC and PCICA features provide cryptographic support for SSL in Linux environments. The crypto support is only available on G5 and higher servers. For Linux environments there is no requirement for ICSF. The software communication to the crypto modules within the features is provided via IBM Linux software driver support.

The Linux for S/390 and zSeries information is available from the following web site:
http://oss.software.ibm.com/developerworks/opensource/linux390/index.shtml
Within the 2.4.7 code drop the recommended OCO 31-bit modules include the crypto modules shown below. Use of "On-demand timer" requires the special timer crypto support listed second. The 64-bit z90crypt is still experimental. Associated with each of the Linux downloads is a MD5 data integrity code.

- z90crypt-2.4.7-s390-2.tar.gz and
- z90crypt-2.4.7-s390-2-timer.tar.gz

Documentation for z90crypt is included in the "LINUX for S/390 Device Driver and Installation Commands" manual. This manual can be reached from the web site listed above. Chapter 7 contains the information on installation and use of the crypto driver, device, and setup of the Apache Web Server with SSL to access the crypto device.

Using z90crypt on VM-guests requires z/VM 4.2 and APAR VM62905.

Reference Tables

Crypto under Linux

Functions or Attributes	PCICC	PCICA
Support Linux SSL handshake exploitation	x[1]	x
Enablement Required via loading of diskette	x	x
Specific Driver level or MCL[2]	38	3CG
Requires CCF active	-	-
Requires ICSF to be active	-	-

[1] If both PCICC and PCICA features installed, only PCICA features will be used within the Linux environment.

[2] Hardware driver levels are listed. See the section immediately prior for information of Linux and VM levels.

Features Differences, Capabilities and Requirements

Functions or Attributes	CCF	PCICC	PCICA
Operating Environments			
Support for Linux applications doing SSL handshakes (requires special device driver and code)	-	x	x
Support for OS/390 applications using ICSF	x	x	-
Support for z/OS applications using ICSF	x	x	x
Hardware available on CMOS G5, G6 servers	x	x	-
Hardware available on z900 servers	x	x	x
Hardware must be explicitly ordered for servers	on z800	x	x
Hardware available on Multiprise 3000 and IBM G4 servers and the withdrawn Multiprise 2000 and IBM G3 servers	x	-	-
Installation	**CCF**	**PCICC**	**PCICA**
Disruptive process to enable	x	-	-
Uses CHPIDs	-	x	x
Requires IOCDS definition	-	-	-
Possible impact to IOCDS due to CHPID order requirements	-	x	x
Physically attached to CP	x	-	-
Requires configuration load before usage	x	x	-
Configuration data storage area[1]	SE	HSA	HSA
Requires CCF active	-	x	x[2]
Requires system master keys loaded	x	x	-
Requires ICSF to be active	x	x	x[2]

Functions or Attributes	CCF	PCICC	PCICA
Requires specific Driver level or MCL	-	x	x
Functionality	**CCF**	**PCICC**	**PCICA**
Offers user programming function support (UDX)	-	x	-
New algorithm expansion	-	x	-
New API function expansion	-	x	-
Usable only for SSL handshake crypto function (decryption of pre-master secret from under server's public key and using clear symmetric key values only)	-	-	x
Supports SSL functions	x	x	x
Usable for data privacy - encryption and decryption processing	x	-	-
Usable for data integrity - hashing and message authentication	x	x	-
Usable for financial processes and key management operations	x	x	-
Provides Highest SSL Handshake Performance	-	-	x
Provides Highest Symmetric Encryption Performance	x	-	-
Crypto RMF Measurements (beginning with z/OS V1R2 and APAR)	x	x	x
Tamper-resistant hardware packaging	x	x	-
FIPS 140-1 certified [Level 4 with secure key entry (TKE)]	x	x	-
System (master) Key storage	x	x	-
Retained Key storage	-	x	-

Legend:
x implies environment is applicable to feature
- implies environment is not applicable or not available

[1] The Configuration Data is loaded into the cryptographic hardware but is also stored external to the crypto devices for loading into either new devices (for PCI features only) or for reloading into devices that may have loss the configuration data.
[2] The function or attribute is not applicable for PCICA in Linux environments.

Summary of Crypto Hardware Ordering Overview

Ordering Issue	CCF	PCICC		PCICA
		G5/G6	zSeries	zSeries
Hardware Feature Indicator	080,[004]	0860	0861	0862
Additional Feature Codes Required to Receive Enablement Diskette for Hdw Feature	x	x	x	-
Server information required for MES order	-	x	x	x
Enablement Required for Feature[1]	x	x	x	-
Charged Feature	x[2]	x	x	x

Ordering Issue	CCF	PCICC		PCICA
		G5/G6	zSeries	zSeries
Prerequisite Operating System Minimum Level	OS/390 V2R4 or OS/390 V1 + ICSF 5655-120	OS/390 V2R9	z/OS V1R1	z/OS V1R2
CCF Configuration Required for OS/390 or z/OS environment	x	x	x	x
Prerequisite minimum hardware microcode level required	-	Driver 38	Driver 38	Driver 3CG EC J10638 + MCLs EC J10645 + MCLs
Maximum Number of Features Available	2 (see TechDoc TD100158)	8	8	6
Use with Linux	-	Linux 2.4.6 + Driver[3] code	Linux 2.4.6 + Driver[3] code	Linux 2.4.6 + Driver[3] code

Legend:

x implies environment is applicable to feature

- implies environment is not applicable or not available

[1] Configuration data allows cryptographic hardware to be functional. Configuration load is done by IBM CE.

[2] CCF Enablement Diskette is a charged feature for Multiprise servers and the IBM G3 server in US. Other countries may have charges on all CCF Enablement Diskette orders regardless of server.

[3]Special driver code is required to use the cryptographic hardware in Linux environments. This driver code provides the programming interfaces for requesting functions to be performed. This code obtained from Linux normal distribution from SuSE.

[4]CCFs are not standard part of processor build for z800, no automatic showing of 0800 feature when ordering processor. Must manually specify 0800 with order if desired, charges may be associated.

Summary of Crypto Hardware CHPID Use

Type of Adjunct Processor	Feature	Number of CHPIDs Required*
PCICC on G5/G6 Servers	0860	1
PCICC on zSeries	0861	2
PCICA on zSeries	0862	2

* Note the number of CHPIDs affected by the installation of the cryptographic hardware may be more than that listed as required due to configuration rules.

Trademarks:

7 zSeries, zSeries 900, z/OS, z/VM, S/370, PR/SM, FICON, and VSE/ESA are trademarks of International Business Machines Corporation in the United States or other countries or both.