

ibm.com



e-business

z/OS 1.2 Cryptographic Services Enhancements



Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2001

IBM

Agenda

➤ **OS/390 Cryptographic Services (OS/390 R7 and above):**

- System SSL
- ICSF (Integrated Cryptographic Services Facility)
- OCSF (Open Cryptographic Services Facility)

➤ **These services are part of the OS/390 - z/OS base**

➤ **These services provide cryptographic functions**

- export/import controlled via selectable feature FMIDs for OCSF and System SSL
- via hardware diskette for ICSF

System SSL Enhancements



Redbooks

International Technical Support Organization

System SSL Overview

✦ Using System SSL, the customer can

- Leverage secure socket communications in their applications (both TCB and SRB mode)
- Create/manage their own digital certificates
- Use RACF digital certificates for secure communications in their applications

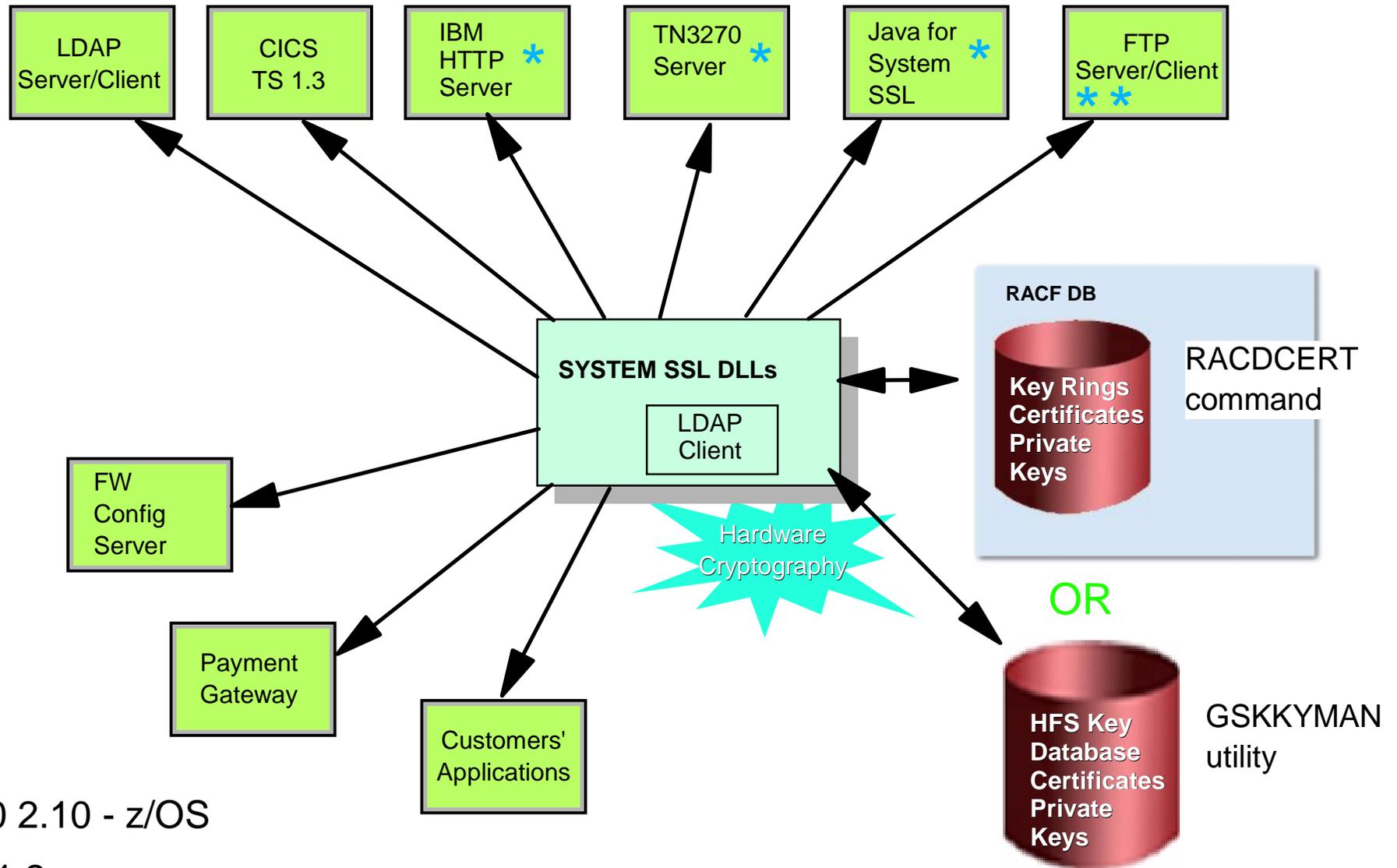
✦ Advantages:

- Saves the customer from providing their own SSL code
- Allows for consolidation of digital certificates in RACF
- Makes use of cryptographic hardware if enabled

✦ Interactions and Dependencies

- Cryptographic hardware is used if ICSF is enabled and running
- OS/390 products using System SSL include: LDAP, Firewall configuration server, CICS, ...

System SSL Overview



* OS/390 2.10 - z/OS

** z/OS 1.2

System SSL V2R7-V1R1 Review

- Introduced in Release 7 as part of the Cryptographic Services element
- Support for Certificate Management through gskkyman
 - key database file in HFS
- External APIs functions for establishing and using SSL socket connections:
 - gsk_initialize
 - gsk_secure_soc_init
 - gsk_secure_soc_read
 - gsk_secure_soc_write
 - gsk_secure_soc_close
- Other utility functions provided:
 - gsk_get_dn_by_label()
 - gsk_get_cipher_info()
 - gsk_free_memory()

System SSL V2R7-V1R1 Review cont'd

- Release 9
 - New APIs
 - gsk_secure_soc_reset
 - gsk_uninitialize
 - gsk_user_set
 - GSKSRBRD and GSKSRBWT(SSL read/write operations while in SRB mode.)

APAR OW47332
- Release 10
 - Limited Java Interface
 - Remove
- z/OS Version 1 Release 1
 - Release 10 functionality shipped.

V1R2 Overview

- **Objectives**

- As industry standards change and more applications exploit the functionality of the SSL cryptography, the need exists to continuously provide functionality to meet the changing standards as well as provide applications flexibility in the utilization of SSL functions. For example,
 - Transport Layer Security (TLS)
 - Multi-environment Support
 - Serviceability
 - Requirements from current exploiters

- **Solution:**

- In V1R2 we upgraded our System SSL functionality to support the industry standard Transport Layer Security (TLS) protocol and introduced a new set of application APIs that provide application with more functionality, flexibility and robustness.

A Word on TLS ...

- The IETF TLS Working Group was established in 1996 to standardize a 'transport layer' security protocol, and in 1999, RFC 2246, TLS Protocol Version 1.0 was published as a Proposed Standard
- TLS work has been based on SSL version 3.0 by Netscape, however the differences between this protocol and SSL 3.0 are significant enough that TLS 1.0 and SSL 3.0 do not interoperate
- Most of the SSL enabled products are in the process of migrating to TLS support as an alternate option to SSL. The same secure ports as SSL are usually used
- Backward compatibility with SSL is supported:
 - ▶ TLS clients who wish to negotiate with SSL 3.0 servers should send client hello messages indicating support of SSL 3.0 and TLS 1.0. The server responds accordingly to the highest protocol it supports
 - ▶ TLS server which agrees to interoperate with SSL 3.0 only clients should accept SSL 3.0 client hello messages and respond with an SSL 3.0 server hello

Upgrade System SSL Functionality

Interactions and Dependencies

- Hardware
 - System SSL will make use of the S/390 Cryptographic Coprocessor feature or PCI Cryptographic Coprocessor if installed and ICSF is running
- Software
 - RACF
 - ICSF
- Exploiters
 - Planned exploiter - Secure FTP
 - Current Exploiters
 - Secure TN3270, HTTPS Webserver, Websphere, Firewall, LDAP, CICS
- Migration and Coexistence
 - All previously built System SSL applications will work.
 - APIs used by application in V1R1 and earlier are being deprecated

Upgrade System SSL Functionality Invocation

■ Upgraded System SSL consists of:

- ▶ Key and Certificate Management functions through the gskkyman command
- ▶ Continued support for keys/certificates created through the RACDCERT command. Allow keys to be stored in ICSF.
- ▶ Hardware Crypto exploitation
- ▶ New set of C/C++ callable functions for establishing and using SSL socket connections
 - TLS
 - certificates
 - "bounced" LDAP
 - allow for multiple SSL environments to be established
- ▶ Continued support for existing external C/C++ callable functions

Certificate and CRL Support

■ Certificates

- ▶ Certificate support based on x.509 Version 3 Certificate standards
- ▶ Limited x.509 PKI Certificate Support
 - RFC 2459
 - Tivoli PKI Trust Authority 3.2.0

■ CRLs

- ▶ CRLs stored in LDAP database
- ▶ CRLs created by the Tivoli PKI Trust Authority

■ Validation

- ▶ Certificate content validated
- ▶ If CRL validation requested, LDAP database query performed to verify certificate has not been revoked. Query performed using the x.500 directory name

Multi-environment Enhancement

■ Enhancement

- ▶ Support more than 1 SSL environment per process

■ Benefit

- ▶ Allow more than one SSL environment to exist
- ▶ Allow for environment attributes to change without destroying existing SSL connections

■ Example

- ▶ One SSL environment supports CRL checking and another does not
- ▶ HFS key database file changes. Start a new SSL environment for new SSL connections and allow existing environment to stay active until connections are gone.

New APIs

- **Primarily 3 categories:**
 - ▶ SSL Environment Management
 - ▶ SSL Connection Management
 - ▶ Miscellaneous

Migrating Existing Applications

V1R1 API Name	V1R2 API Name
<code>gsk_initialize()</code>	<code>gsk_environment_open()</code> <code>gsk_attribute_set...()</code> <code>gsk_attribute_set_callback()</code> <code>gsk_environment_init()</code>
<code>gsk_secure_soc_init()</code>	<code>gsk_secure_socket_open</code> <code>gsk_attribute_set...()</code> <code>gsk_secure_socket_init()</code>
<code>gsk_secure_soc_read()</code>	<code>gsk_secure_socket_read()</code>
<code>gsk_secure_soc_write()</code>	<code>gsk_secure_socket_write()</code>
<code>gsk_secure_soc_close()</code>	<code>gsk_secure_socket_close()</code>
	<code>gsk_environment_close()</code>

ICSF Enhancements



The S/390 Integrated Cryptographic Coprocessors

- **1994 : S/390 CMOS Cryptographic Coprocessor Facility (CCF)**

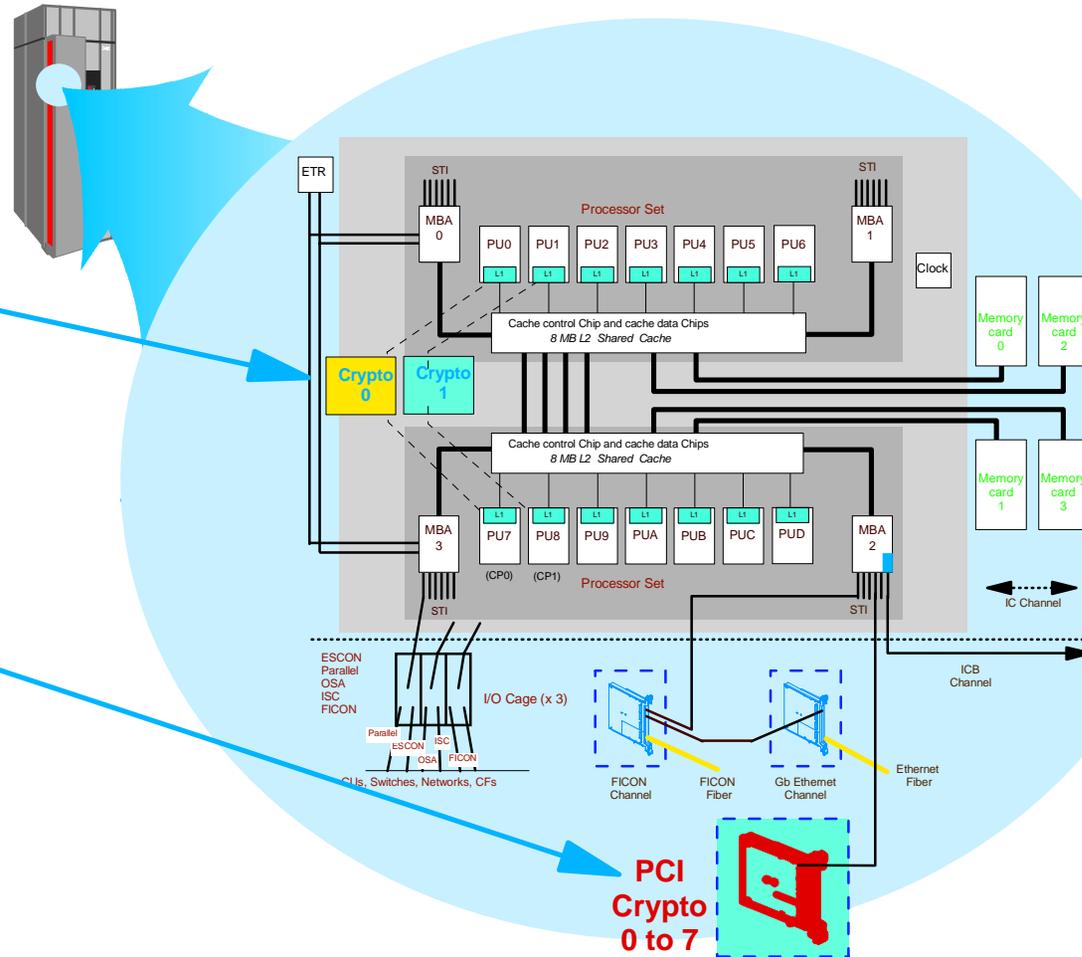
- ▶ priced feature on 9672 G3
- ▶ standard feature on 9672 G4, G5, G6, z900 MP2000, MP3000

- **2000 : S/390 PCI Cryptographic Card (PCICC)**

- ▶ priced feature on 9672 G5, G6, z900
- ▶ 0 to 8 cards in a system

- **2001 : PCI Cryptographic Accelerator (PCICA)**

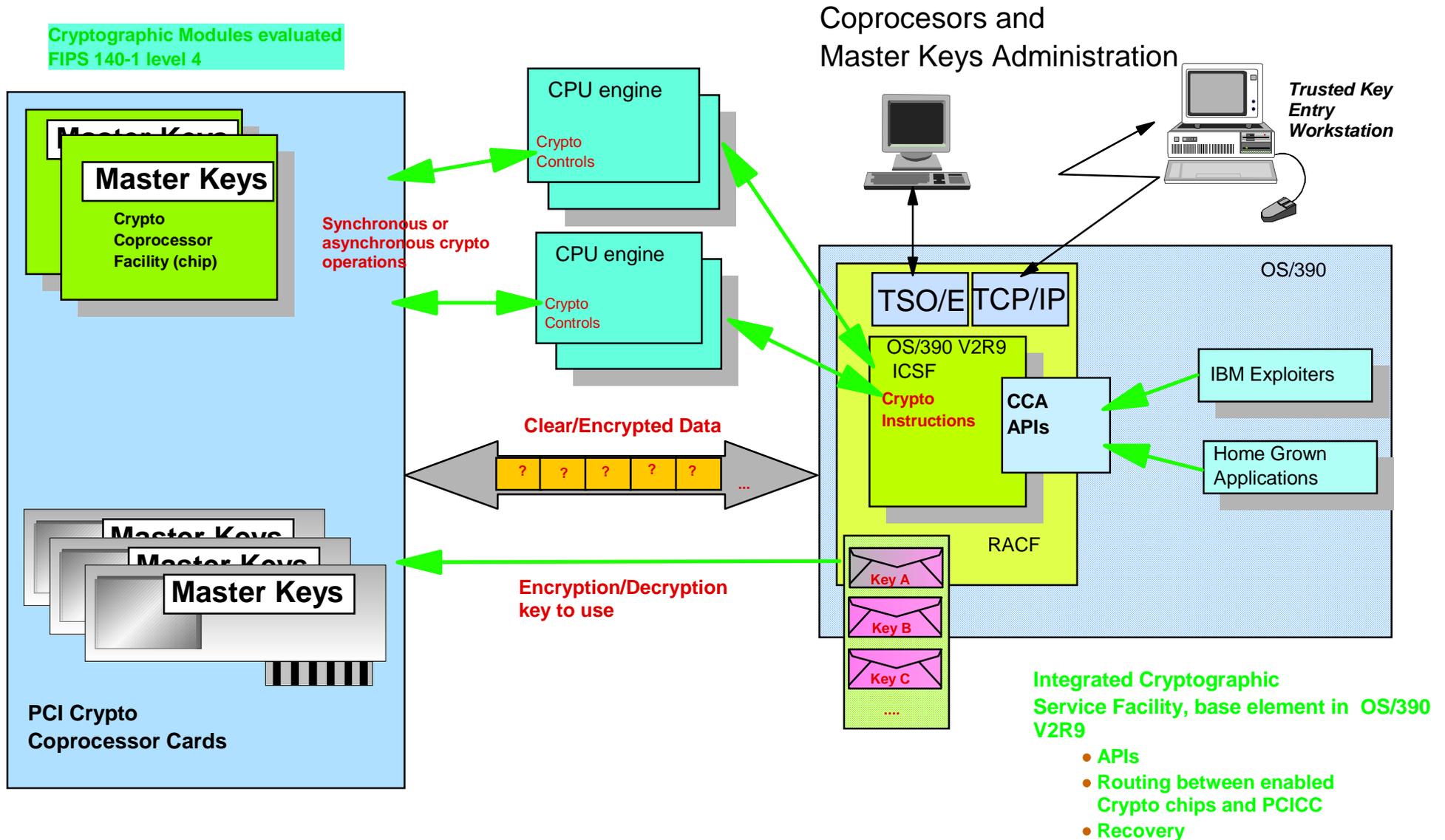
- ▶ priced feature on z900
- ▶ High performance SSL assist



IBM CCA compliant ...

FIPS 140-1 Level 4

The S/390 Integrated Cryptographic Coprocessors



Usability Enhancements

- A number of changes will be made to enhance ICSF
 - ▶ ABENDs replaced with messages
 - ▶ Confusing messages eliminated
 - ▶ MAXLEN parameter checking eliminated
 - ▶ DOMAIN parameter optional
 - ▶ Pass Phrase Initialization enhanced
- ICSF will provide support for customers to develop their own PCICC User Defined Extensions

PKDS Reencipher

ICSF will support the ability to change the PKA master keys

- new TSO utility to reencipher the PKA Key Data Set
- new utility program CSFPUTIL
- PKA Key Token Change callable service

ICC Financial Services

ICCSF will provide services for emerging integrated circuit card standards to support smartcard financial applications.

- Secure Messaging for Keys callable service
- Secure Messaging for PINs callable service

ICC Financial Services

- Secure Messaging for Keys (CSNBSKY)
 - ▶ Encrypts a text block including a clear key value decrypted from an internal or external DES token.
 - ▶ The encryption mode may be either CBC or ECB.
- Secure Messaging for PINS (CSNBSPN)
 - ▶ Encrypts a text block including a clear PIN value recovered from an encrypted PIN block.
 - ▶ The encryption mode may be either CBC or ECB.
 - ▶ The PIN block may be reformatted.

SSL Performance Enhancements

ICSF will provide a performance enhancement for SSL applications

- PCI Cryptographic Accelerator support
- PKDS Cache support
 - PKDSCACHE(n) is a new options data set keyword. n is an integer from 0 to 256 indicating the number of records to be used for the PKDS Cache. The default value is 64.

z900 Integrated Cryptography Performance

- 2 x CCF
- These figures comprise the ICSF path length

• ICSF/API Performance (z900)

– DES CBC	80 MB/sec
– TDES (2,3)	48MB/sec
– SHA-1 Hash	43 MB/sec
– RSA SigGen 1024b	104/sec

G6 with 2 CCF + 8 PCICCs : above 1000 SSL handshakes/sec
as SSL server (private key operations)

z900 with 2 CCF + 16 PCICCs : projected above 2000 SSL handshakes/sec

z900 PCICA : 1000 SSL handshakes per second per coprocessor