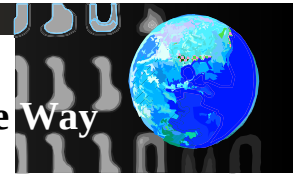


IBM's S/390 Enterprise Server Cryptographic Products

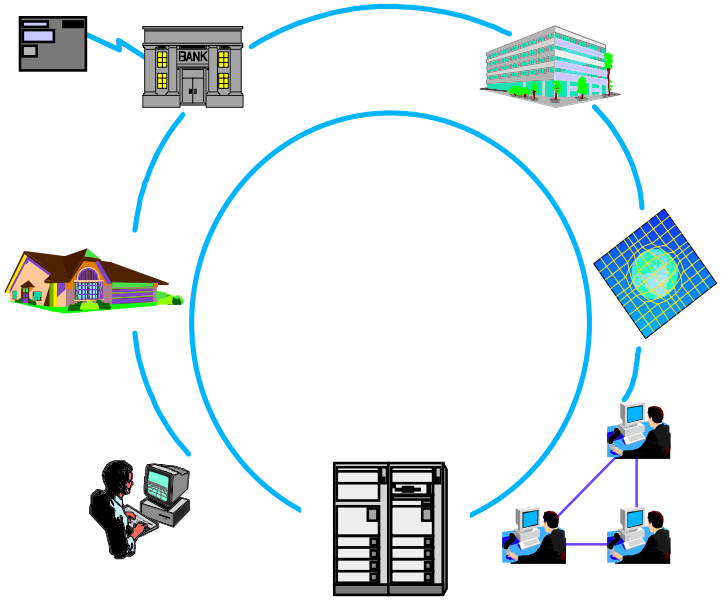
- ***Integrated Cryptographic Feature***
- ***CMOS Cryptographic Coprocessor Facility***

Today's Electronic World

SecureWay

Threats

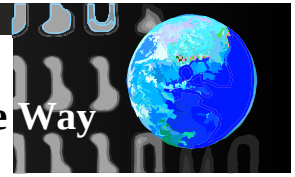
- Errors
- Theft
- Fraud
- Wiretaps
- Competitors
- Terrorists
- Dishonest insiders



Countermeasures

- Identification
- Access control
- Auditing
  - Cryptography

Applications & Concerns



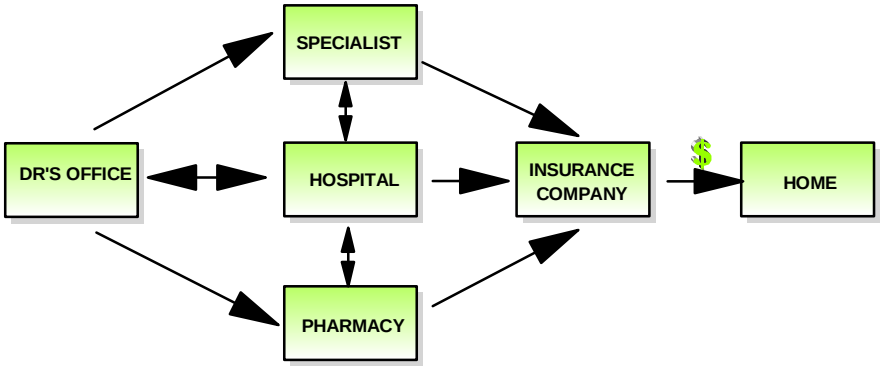
- Confidentiality/Privacy
  - Protecting Information from unauthorized disclosure or viewing during both data storage and network transmission
- Integrity
  - Ensuring that the information arriving is the same as the information that was sent
- Accountability (Nor-Repudiation)
  - Proving that a transaction actually occurred
- Authentication
  - Proving that a resource (human or machine) is what it claims to be

Cryptography alone can provide security for the information flowing on the Network and a guarantee of its receipt

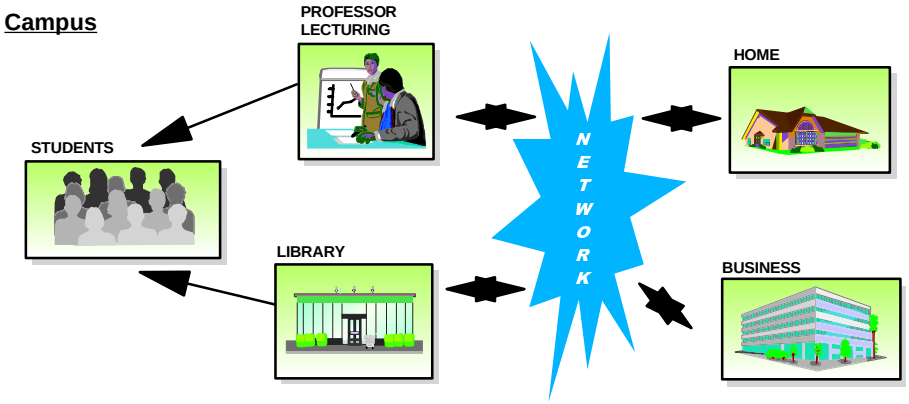
Added Value of Cryptography

Secure Way

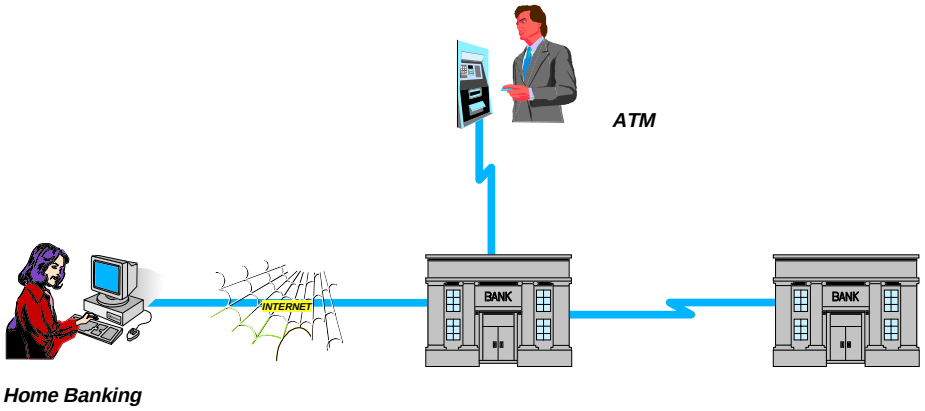
Healthcare



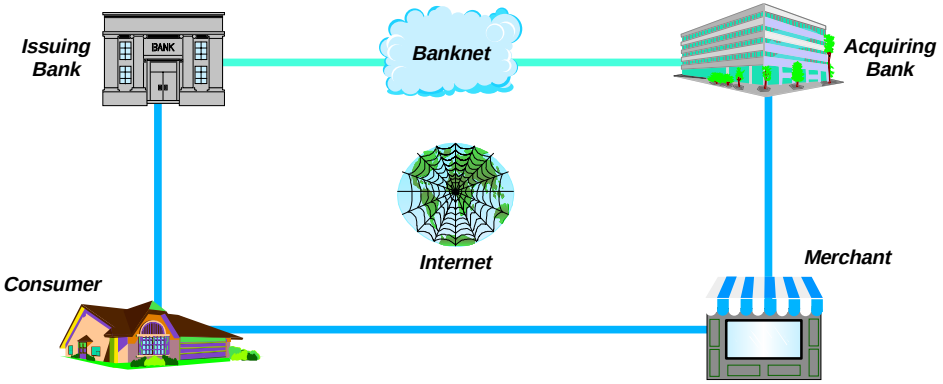
Education

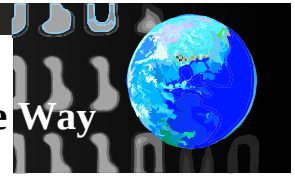


Finance



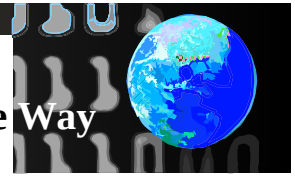
E-Commerce



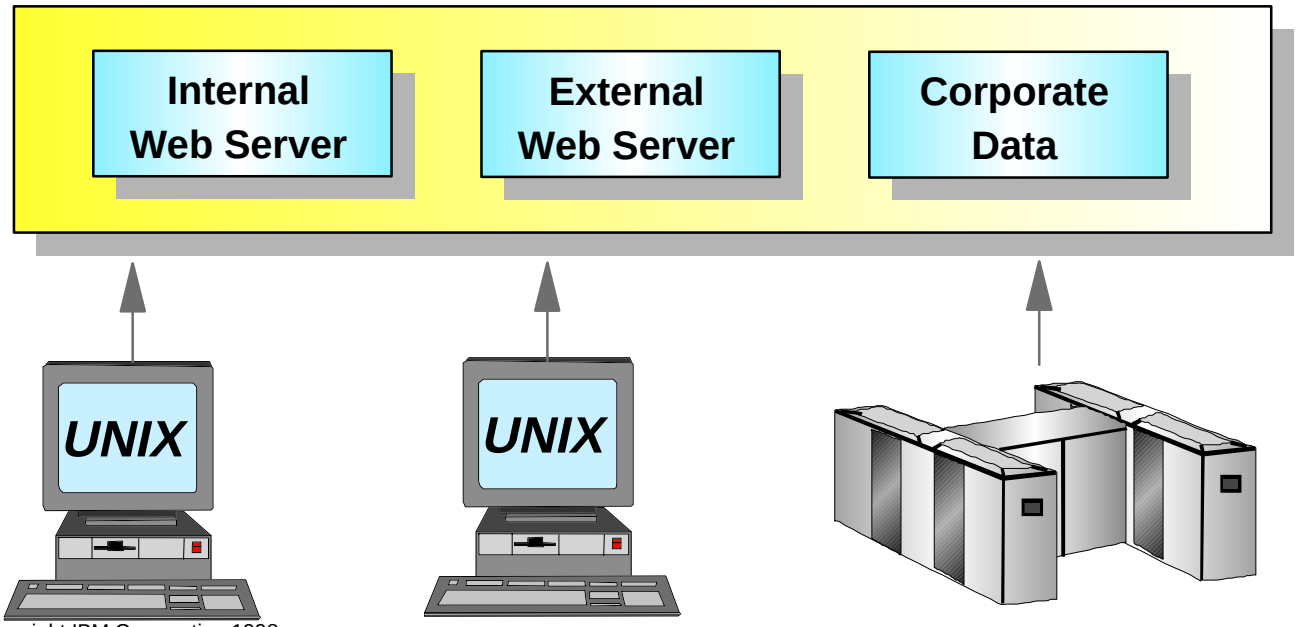


- **Electronic Commerce will:**
  - Open new delivery methods for goods & services
  - Radically redefine the global financial systems
  - Significantly reduce costs
  - Expand market reach by reducing entry barriers
  - Minimize the compartmentalization of knowledge
- Provided a reliable and cost effective solution is available that will:
  - Authenticate receipt
  - Assure confidentiality
  - Guarantee integrity
  - Protect intellectual property
  - Provide for selective application

S/390 Enterprise Server w/Cryptographic Coprocessor



- **Exploits classic strengths**
  - Scalability
    - Data Volume
    - Transaction Volumes
  - System Integrity
- **Open Computing**
- **Allows cost effective secure IT Structure**



S/390 SERVER
"Single System"

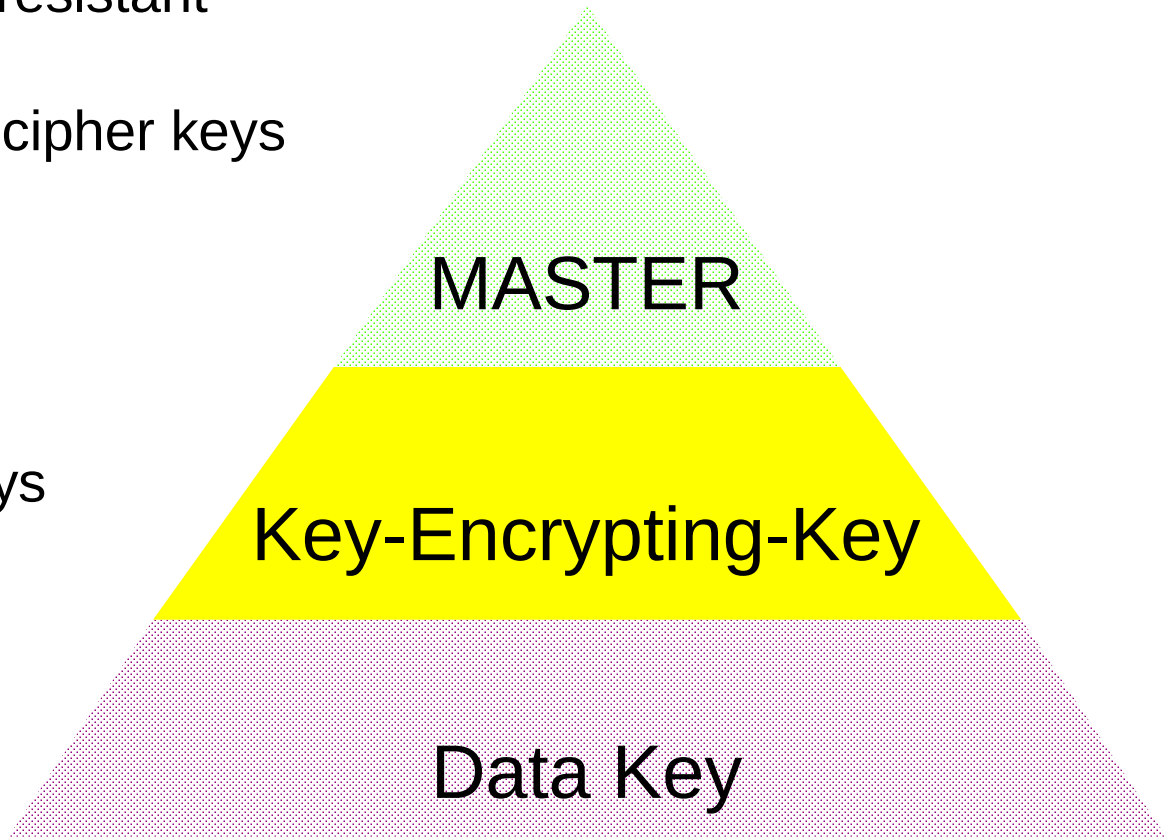
Vs.

Separate
Platforms

Cryptographic Key Hierarchy

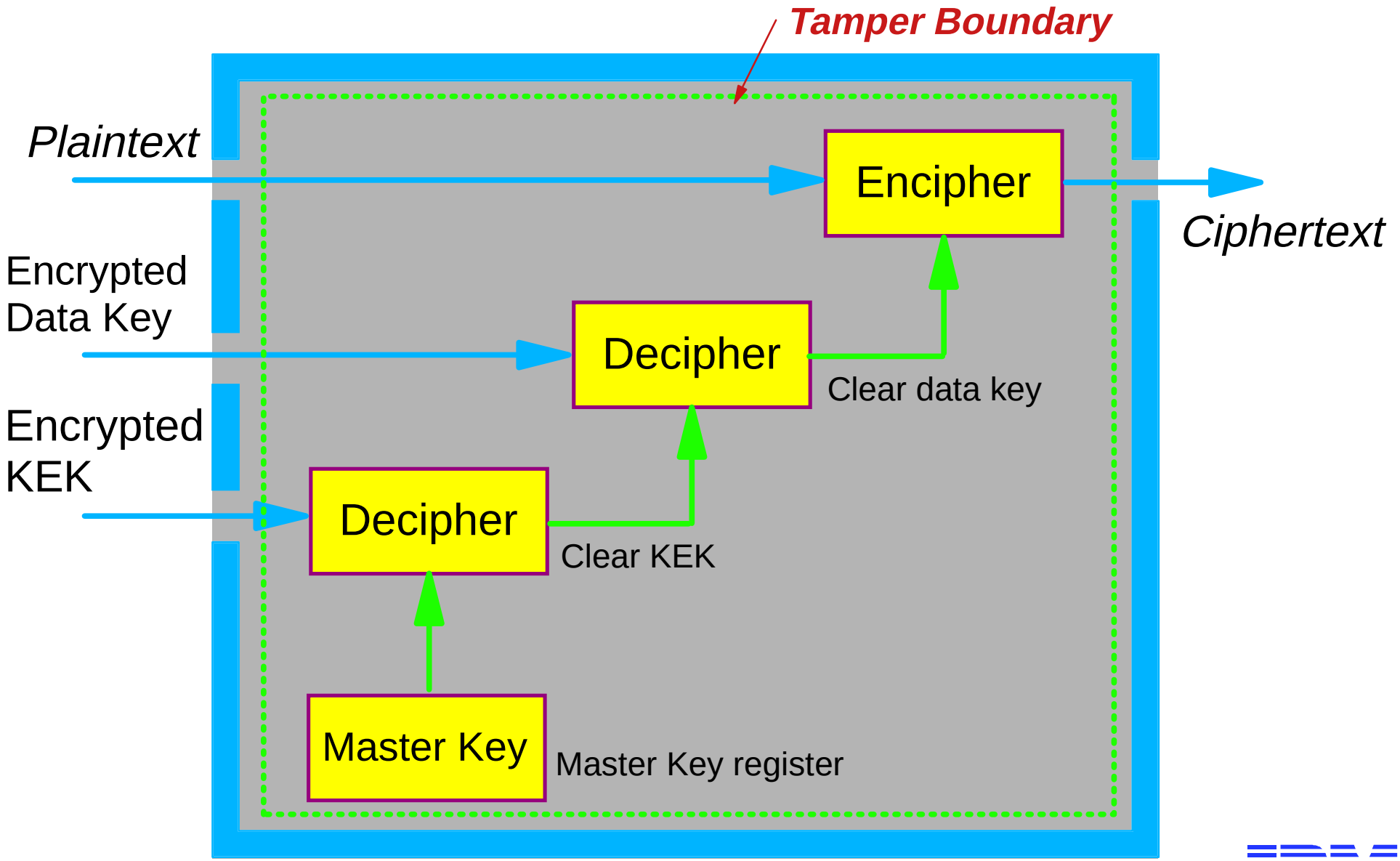
Secure Way

- MASTER
  - Protected within tamper resistant hardware
  - Used to encipher and decipher keys
- Key-Encrypting-Key
  - Stored in a file
  - Used to protect other keys
- Data Key
  - Stored in a file
  - Used to protect data



IBM®

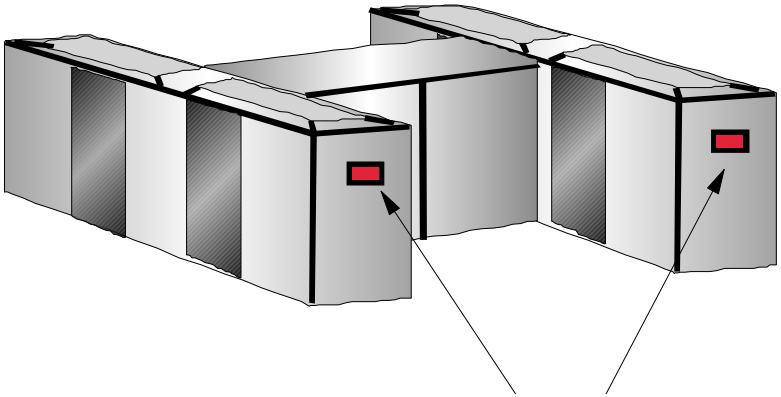
Tamper Resistant Hardware



IBM ES/9000-9021
Integrated Cryptographic Feature (ICRF)

Secure Way

ES/9000-9021

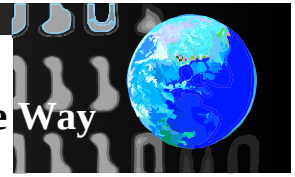


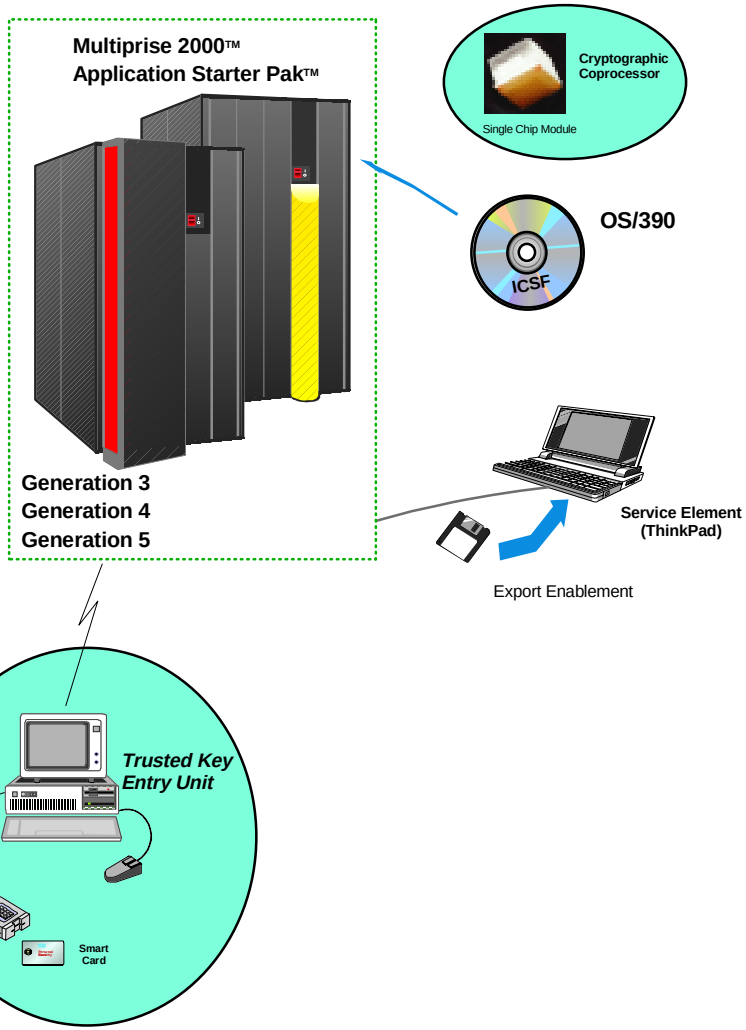
ICRF

High Performance
FIPS 1027 Physical Security

- Data Privacy
  - FIPS 46-1 DES (56 bits)
- Data Integrity
  - Message Authentication Code
- Authentication
  - PIN Functions
- Key Management
  - Triple DES
- LPAR Support
- Manual Master Key Entry
  - SmartCard
  - KeyPad

IBM S/390 CMOS Cryptographic Coprocessor



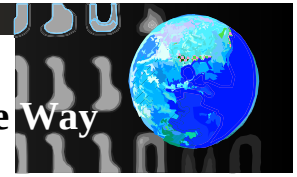


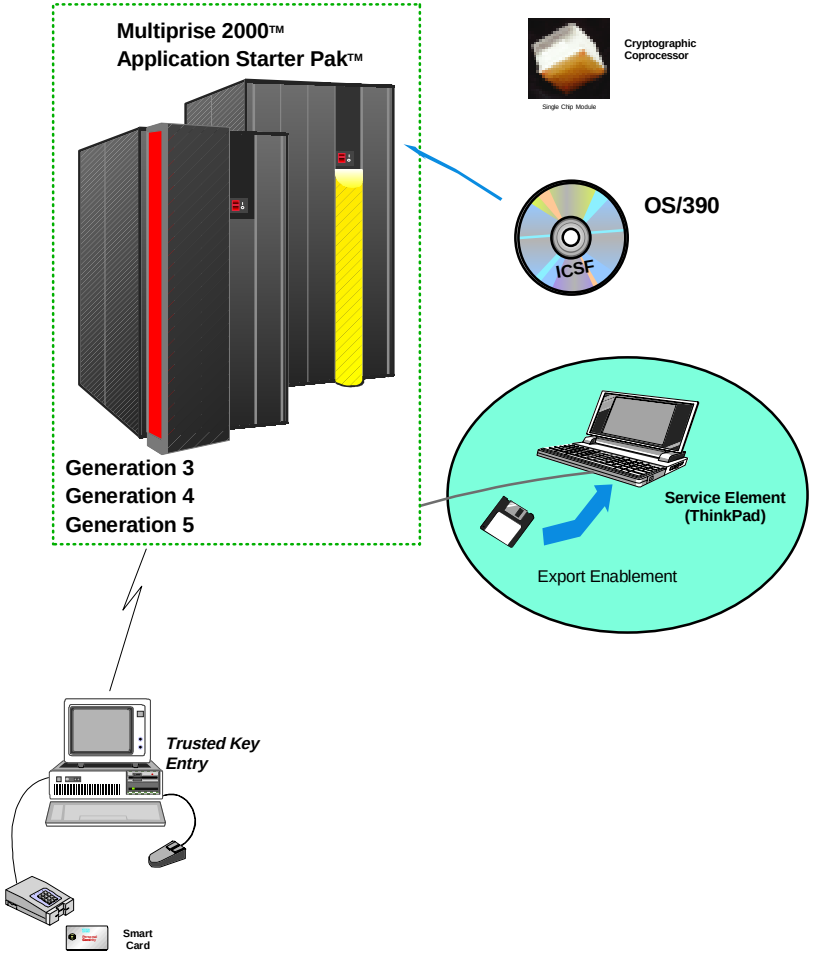
- ✓ Off-Load Cryptographic Coprocessors
- ✓ Negligible CP Utilization
- ✓ Concurrent CP/DES/PKA Execution

Security Function Highlights

- **Data Privacy**
  - Data Encryption Standard
    (DES) [56 bits]
    (TDES) [168 bits]
  - Commercial Data Masking Facility (CDMF) [40 bits]
- **Data Integrity**
  - Secure Hash functions
    (MDC, MD5, SHA-1)
- **Authentication**
  - PIN Algorithms
  - Message Authentication Code
    (Single Key MAC)
    (Double Key MAC)
- **Non-repudiation**
  - Digital Signature (RSA/DSS)
- **Public Key Algorithms (RSA / DSS / Diffie-Hellman)**
- **Optional Trusted Key Entry (TKE)**
  - Uses public key cryptography and TDES to enforce multiple authority control and loading of Master Keys
- **Security**
  - FIPS 140-1 Validated Level 4 -- Certificate #40
- **LPAR**
- **Fault Tolerant / High Availability**
- **Standard on All S/390 Servers starting with G4**
- **Exportable Hardware / Configurable / Programmable w/CP**

IBM S/390 CMOS Cryptographic Coprocessor *cont.*





US Federal Government Export Control

- **Three "Standard" Configurations**
  - Commercial Data Masking Facility (CDMF)
    Exportable-anywhere without special license
  - Single Key DES [56-bits]
    World Wide under KMI license
  - Triple Key DES [up to 168 bits]
    World Wide - Banks under 'blanket' license
- **Export Level Enabled via Enablement Diskette**
  - Diskettes are uniquely 'tied' to Crypto chip serial number for Export Control

IBM S/390 CMOS Cryptographic Coprocessor Performance

Secure Way

CMOS Cryptographic Coprocessor *Single Chip* Performance

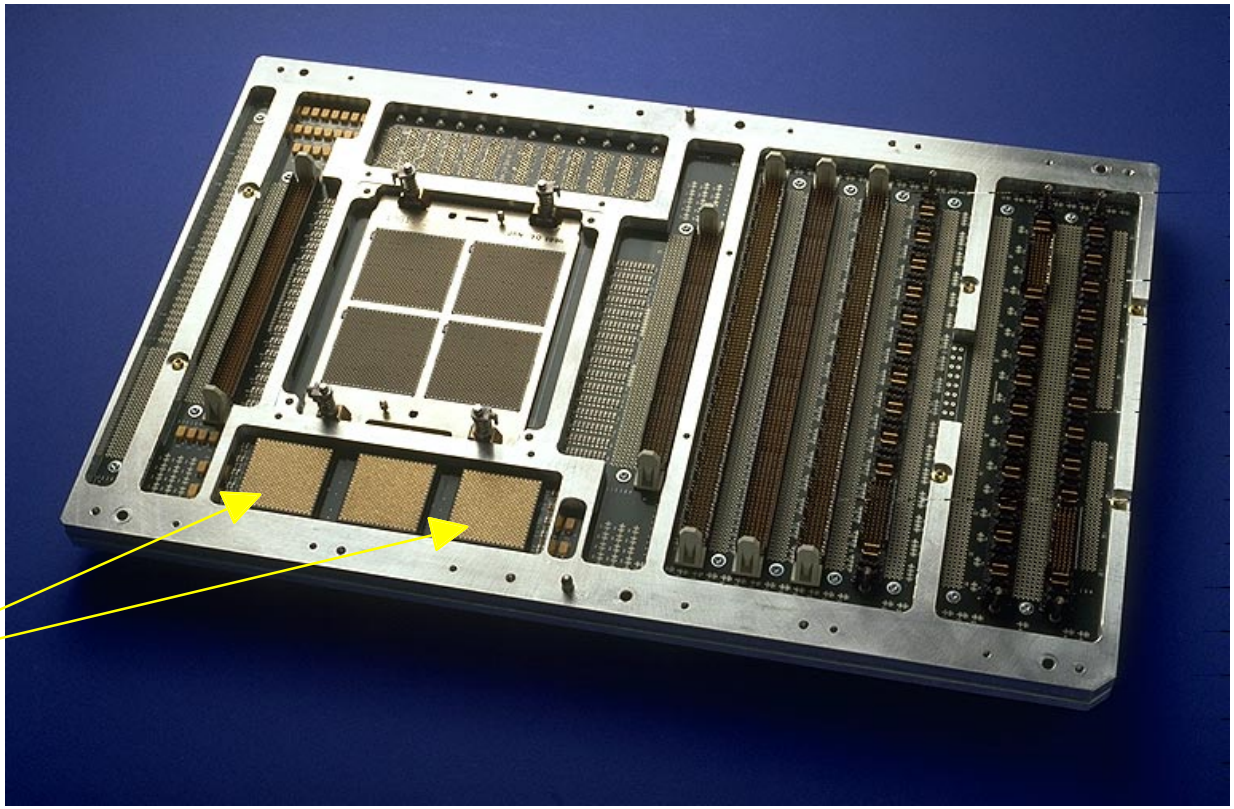
- **DES** 100 MB/sec [CBC]
- **RSA** 77 1024b RSA SigGen/sec [random exponent - no CRT]
  35,325 1024b RSA SigVer/sec [17b exponent - no CRT]

G5 10-way with 2 Crypto Chips, *ICSF API* Performance

- **DES** 56 MB/sec [1MB blocks - CBC]
  30,000 calls/sec [64byte blocks - CBC]
  25,000 calls/sec [64byte blocks - CBC] TDES
- **SHA** 35 MB/sec
- **MAC** 88 MB/sec
- **RSA** 154 1024b SigGen/sec [random exponent - no CRT]
  1970 1024b SigVer/sec [17b exponent - no CRT]
- **DSS** 810 1024b SigGen/sec
  462 1024b SigVer/sec

IBM S/390 CMOS Cryptographic Coprocessor
G3 and G4 Physical Implementation

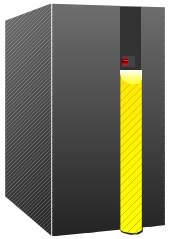
Cryptographic Coprocessor
Single Chip Module (SCM)

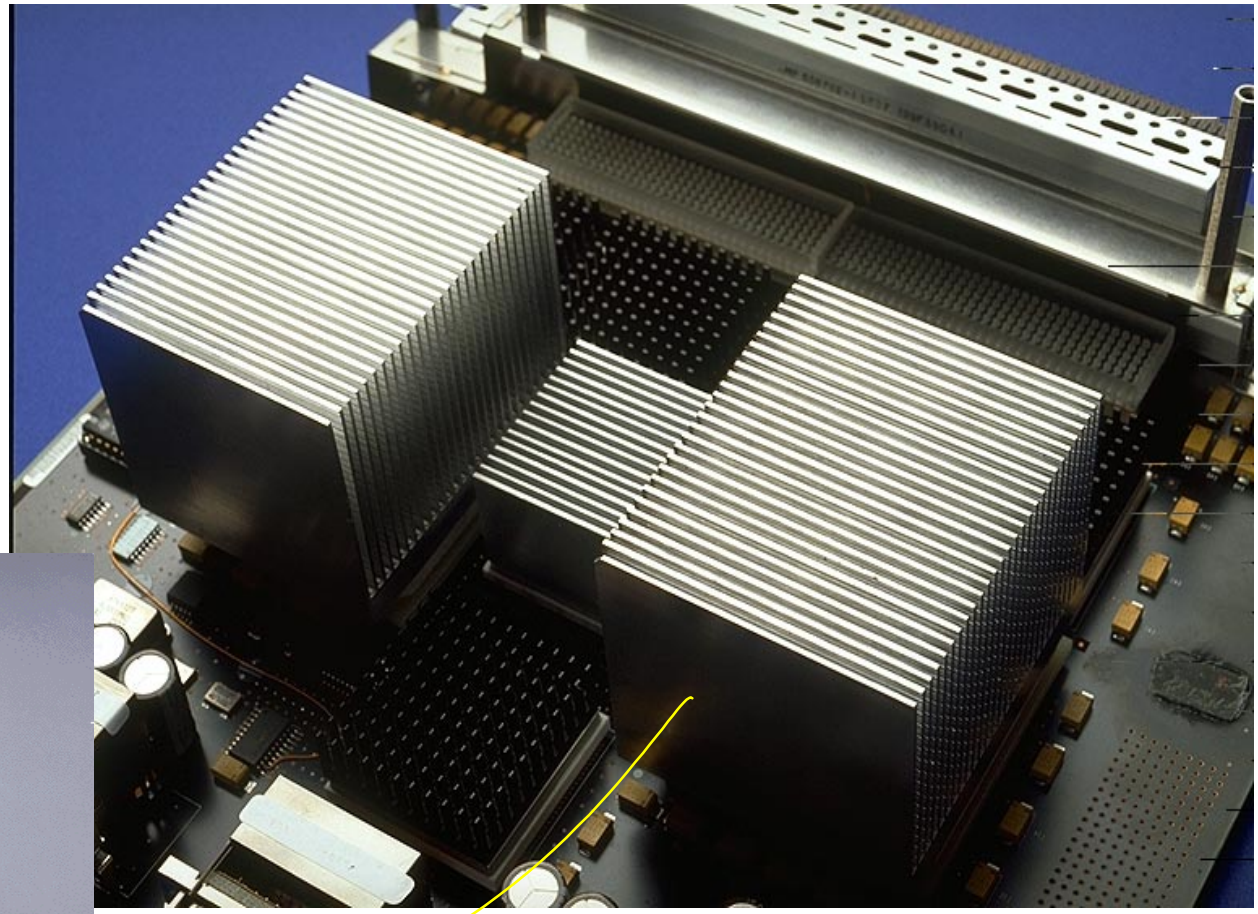


S/390 Processor Board

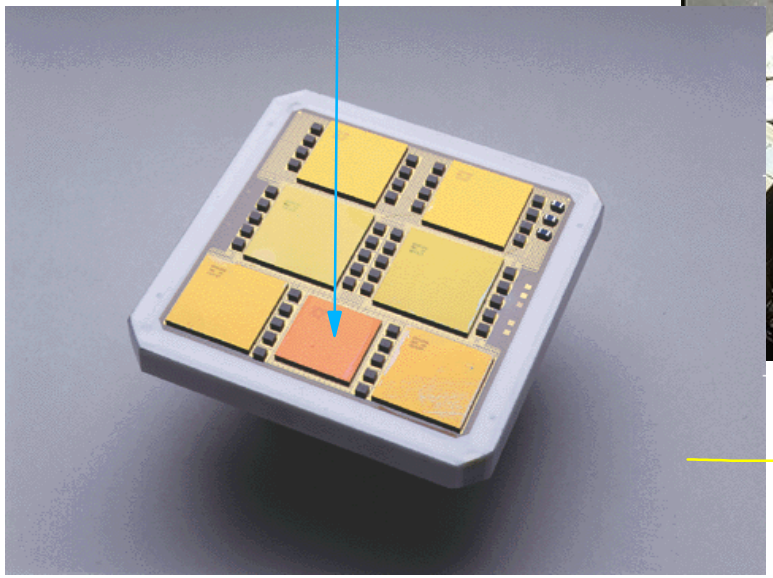
IBM S/390 CMOS Cryptographic Coprocessor
Multiprise 2000™ and Application StarterPak™

Secure Way





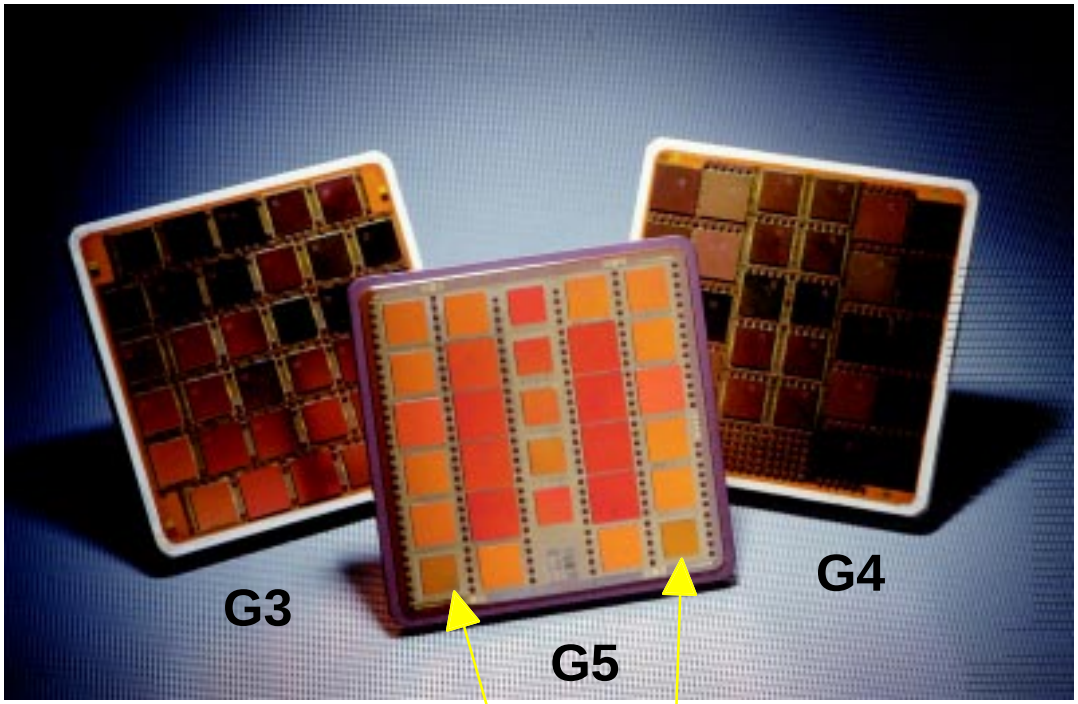
Cryptographic Coprocessor
Single Chip



IBM®

IBM S/390 CMOS Cryptographic Coprocessor
G5 Physical Implementation

Secure Way



Cryptographic Coprocessor
Single Chips

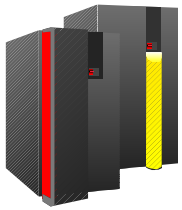
IBM Cryptographic Products

Secure Way

Cryptographic Engines

S/390 CMOS Cryptographic Coprocessor

G3 G4 G5

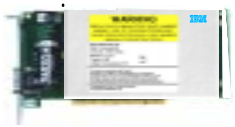


Cryptographic Coprocessor

OS/390

06/97

4758 PCI Cryptographic Adapter



08/97

Transaction Security System

4754

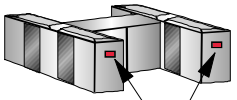
4755

- DOS
- OS/2
- RS/6000
- AS/400

1989

4753

ES/9000-9021



ICRF

MVS

09/90

Common Cryptographic Architecture

- DES
- CDMF
- RSA
- DSS

Other Crypto Products

- Cryptolope Containers
- Lotus Notes
- Public Key Infrastructure
- Certificate Mgmt. Services
- Firewall
- KeyWorks