IBM Systems z

System z – Enterprise Security Hub

Mary E. Moore
IBM System z Security Program Manager

9-Nov-07

Agenda

- System z Security Strategy
- Securing Data for the Enterprise
- System z Security features
  - **Integrity and virtualization**
  - **Network security**
  - **Encryption solutions**
- Security Directions

System z Security

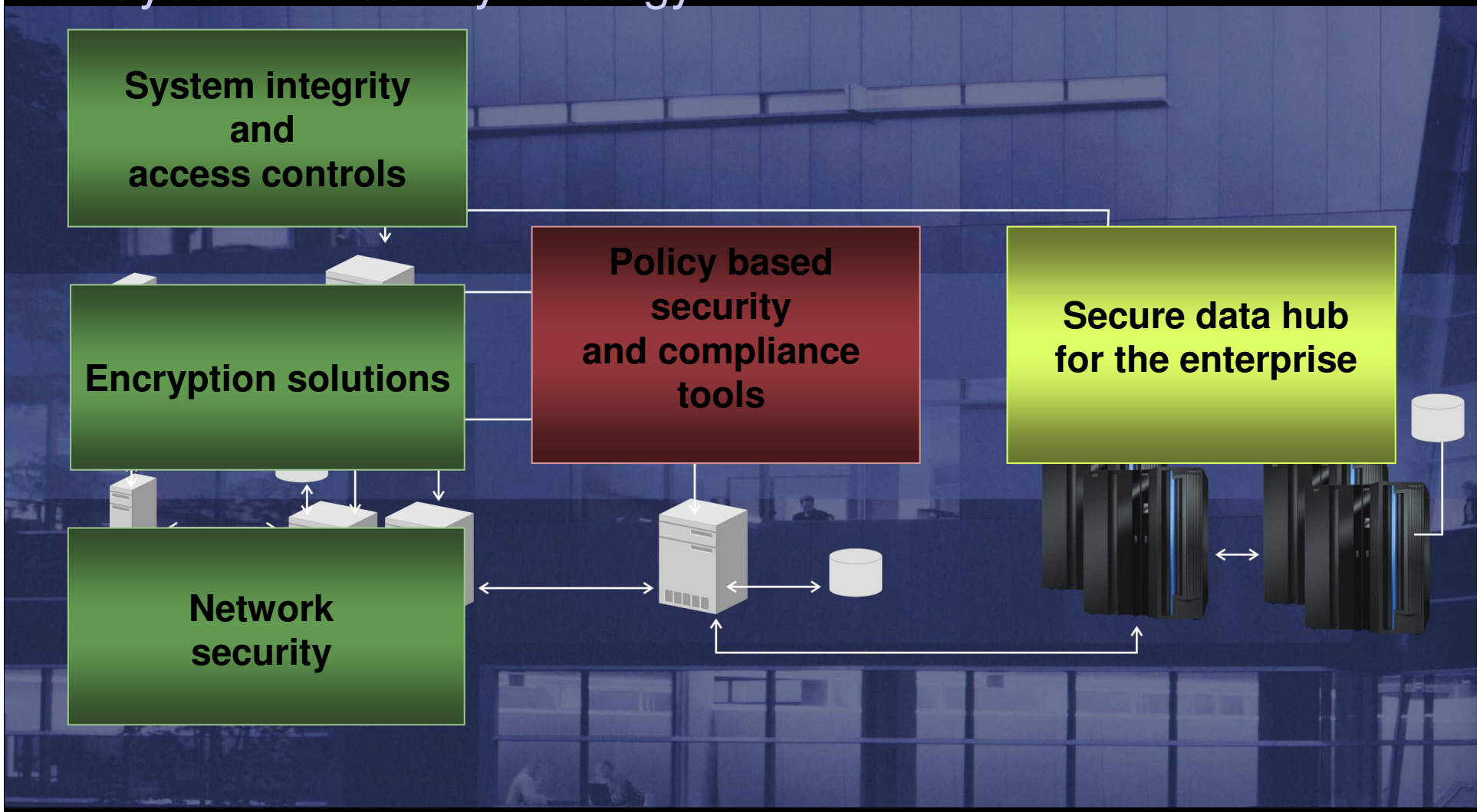
Mitigating the risk of security breaches

Helping to reduce the complexity and cost of enterprise security solutions

Robust security to enable consolidation

- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Encryption solutions to help secure data from theft or compromise
- Highly secure network security
- Allowing you to address compliance needs with more confidence

Managing risk across the enterprise
System z Security Strategy

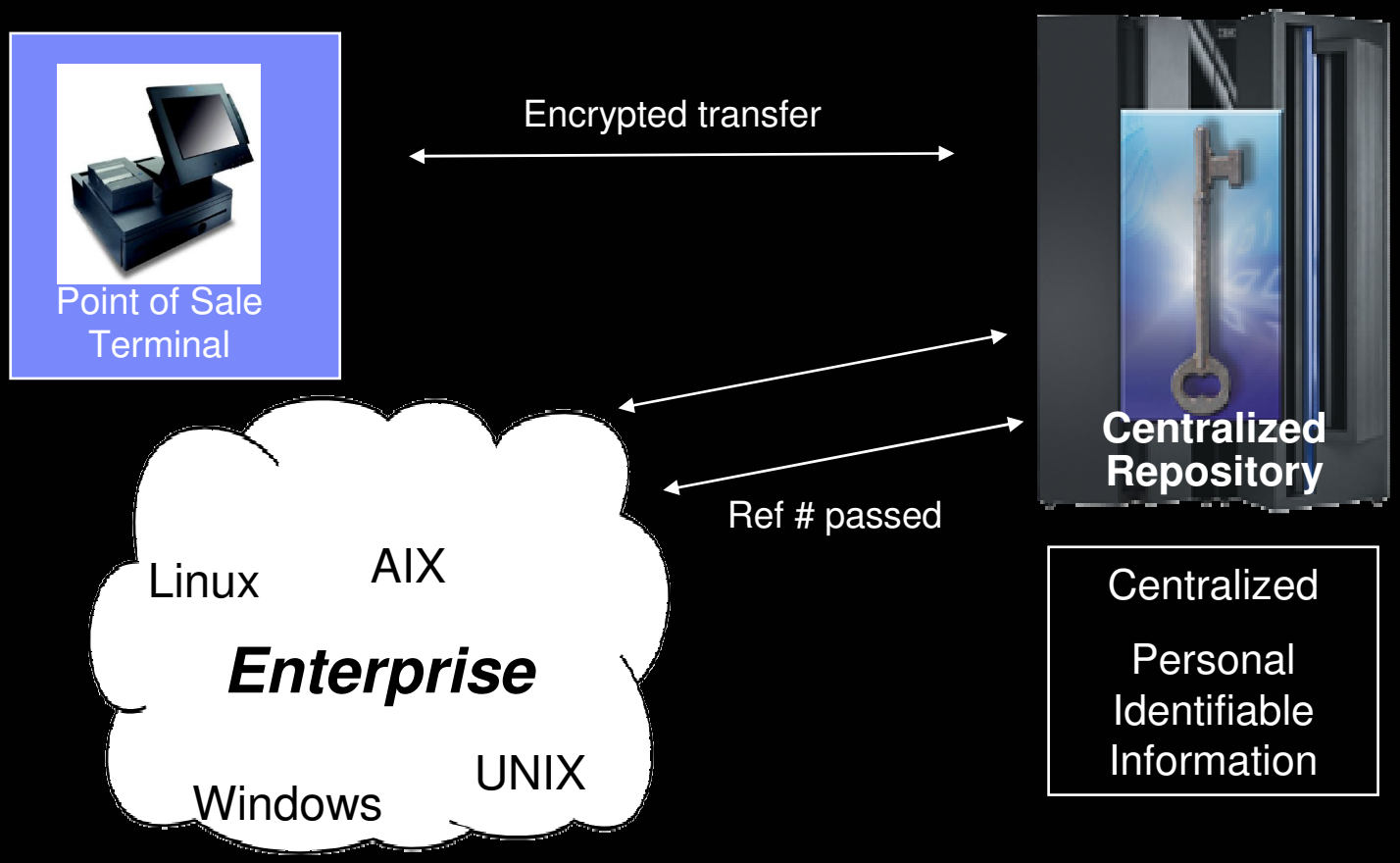


System z as a central repository for sensitive data

Leverage the mainframe policies and processes that have been developed over many years in your enterprise

Minimize proliferation of sensitive data throughout enterprise

Customer Example:
Centralizing and Protecting Sensitive Credit Card Data



Payment Card Industry
PCI DSS Requirements "The Digital Dozen"

Build and Maintain a Secure Network	
1.	Install and maintain a firewall configuration to protect cardholder data
2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
3.	Protect stored cardholder data
4.	Encrypt transmission of cardholder data sent across open, public networks
Maintain a Vulnerability Management Program	
5.	Use and regularly update anti-virus software
6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
7.	Restrict access to cardholder data by business need-to-know
8.	Assign a unique ID to each person with computer access
9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
10.	Track and monitor all access to network resources and cardholder data
11.	Regularly test security systems and processes
Maintain an Information Security Policy	
12.	Maintain a policy that addresses information security – Connected Entities and Contracts

PCI DSS Ver. 1.1

Payment Card Industry Compliance– How System z can help

Build & Maintain a Secure Network

System z integrity features

z/OS Network Policy Agent

z/OS Intrusion Detection Services

Linux on z as a DMZ

Protect Cardholder Data

Encryption Infrastructure

Database Encryption & Test Tools

Network encryption:

SSL/TLS, IPSec, OpenSSH

Tape encryption

Maintain Vulnerability Mgmt Program

z/OS Network Policy Agent

z/OS Intrusion Detection Services

IBM Internet Security Solutions

System z integrity features

RACF and MLS

Tivoli zSecure

Tivoli Identity Manager

Implement Strong Control Measures

z/OS Healthchecker

Tivoli zSecure

Tivoli Compliance Insight Manager

IBM Services:
Penetration Testing

Monitor & Test Networks

z/OS Network Policy Agent

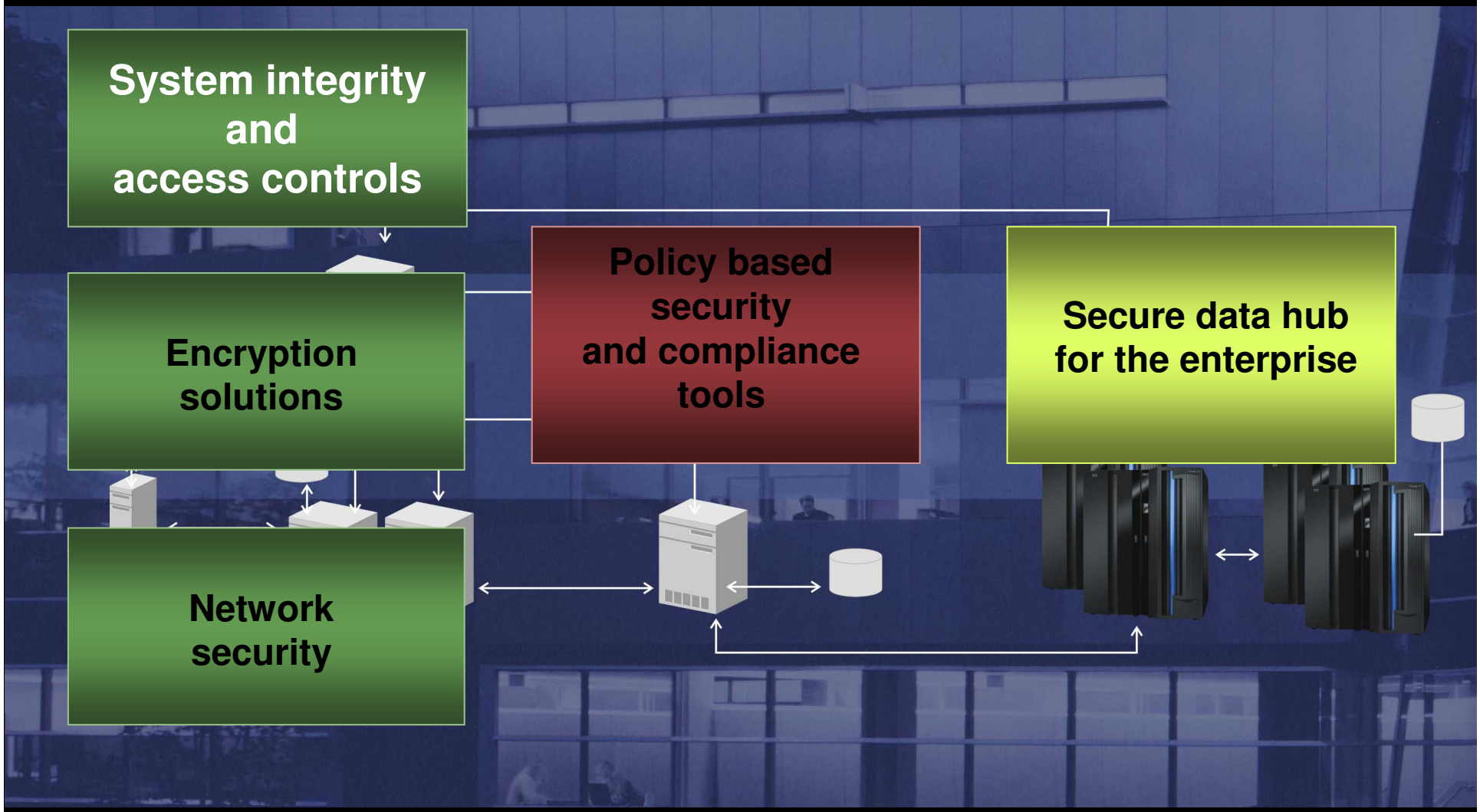
EAL & FIPS Certifications

IBM Services:
Internet Security Solutions
Security & Privacy Consulting

Maintain Information Security Policy

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Managing risk across the enterprise



System z Architecture:
Security Built In By Design

Security is only meaningful in the presence of system integrity!

- Integrity prevents bypass of security controls
- Audit trail confirms conformance

- **Integrity through Hardware and Software integration**
  - Storage protect keys
  - Virtual storage management
  - User isolation

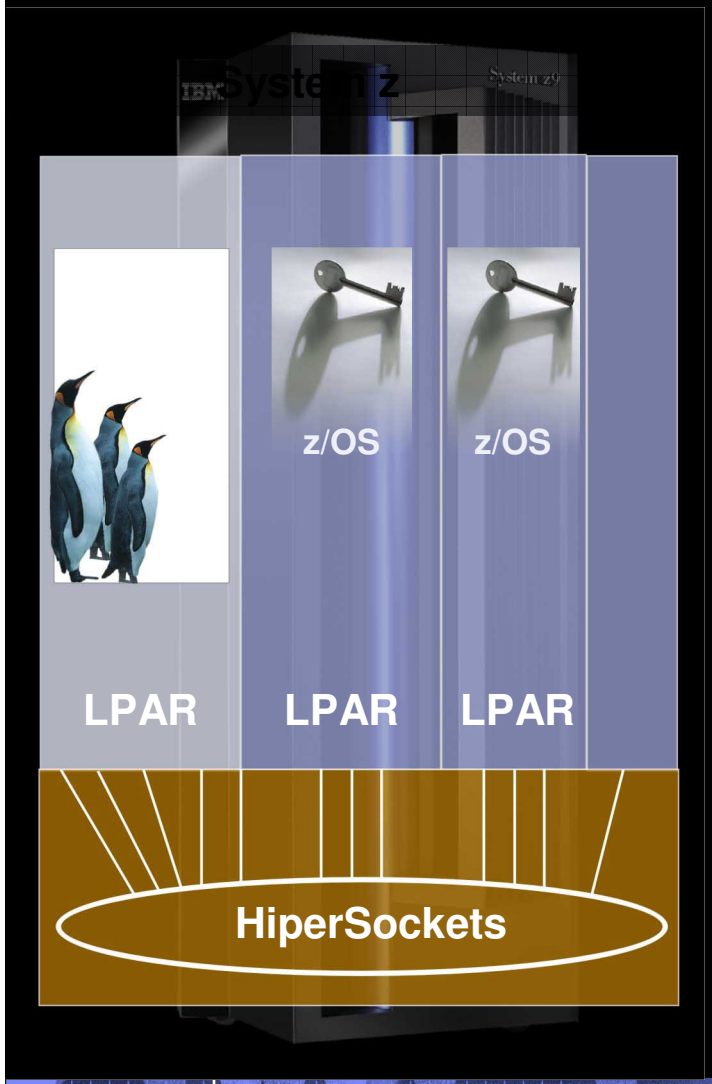
Allows customers to confidently place critical workloads on single z/OS image

and hundreds of Linux images in a virtual partition

Can help prevent intrusion from malware, viruses and worms

Proven over 40 years of secured operations!

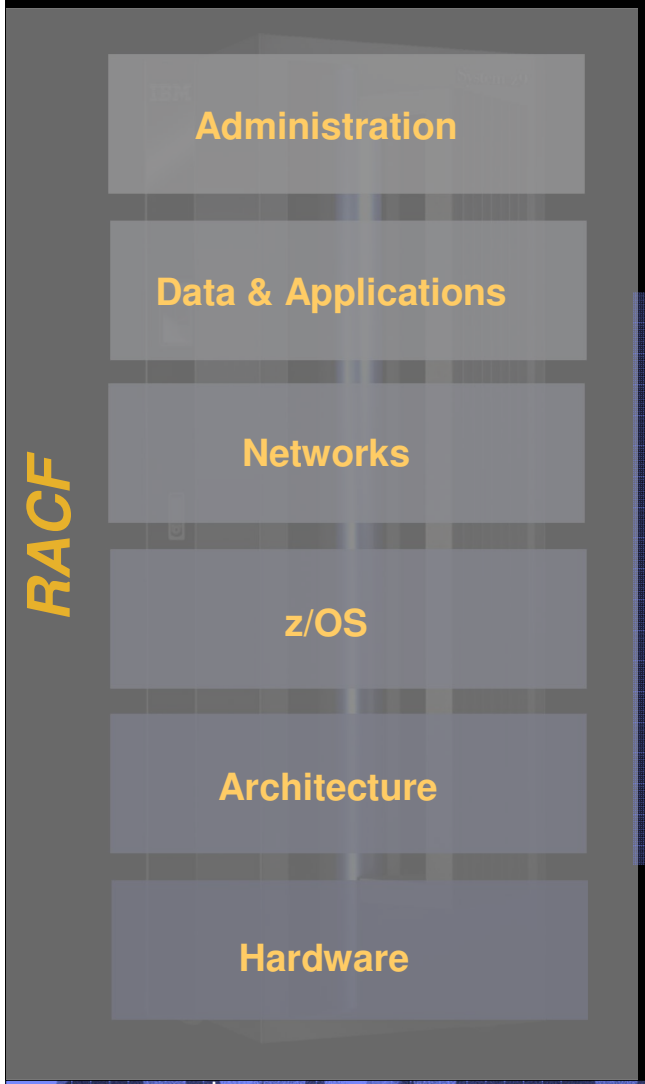
Security through virtualization



- **Virtual servers on a single mainframe: Logical Partitions (LPAR)**
  - **Flexible dynamic provisioning of hardware resources**
  - **Highest Common Criteria certification for server virtualization – EAL5**
- **Virtual network in the server: HiperSockets**
  - **Provides an integrated TCP/IP network through system memory**
  - **Enables a "Data Center" inside a box with a mixture of z/OS and Linux images.**
  - **Highly secure connection – no external network exposed**

The backbone of mainframe security
Resource Access Control Facility (RACF)

Authentication
Authorization
Administration
Auditing



Enables application and database security without modifying applications

Can reduce security complexity and expense:

- **Central security process that is easy to apply to new workloads or as user base increases**
- **Tracks activity to address audit and compliance requirements**

z/OS System Integrity Statement

Designed to help protect your system, data, transactions, and applications from accidental or malicious modification

- **System integrity is the inability to bypass the lock on system resources**
- IBM reaffirms its commitment to z/OS system integrity
- IBM will always take action to resolve if a case is found where the above can be circumvented

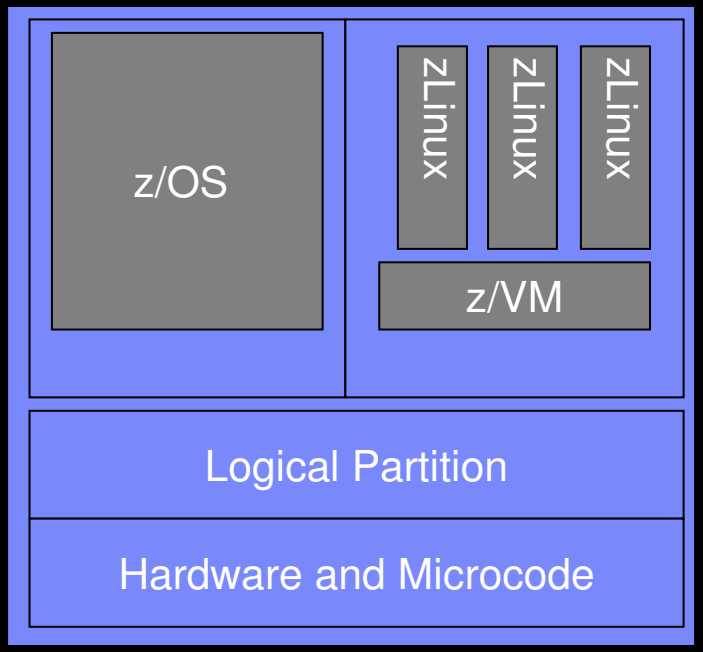
z/OS integrity statement and the Common Criteria certifications can be helpful proof points in addressing compliance requirements.

ibm.com/servers/eserver/zseries/zos/racf/zos_integrity_statement.html

Certifications on System z

z/OS

- **Common Criteria EAL4+**
  - with CAPP and LSPP
  - z/OS 1.7 + RACF
  - z/OS 1.8 + RACF
- **IdenTrust™ certification** for z/OS as a Digital Certificate Authority (PKI Services)



z/VM

- **Common Criteria** EAL3+
  - with CAPP
  - **z/VM 5.1 + RACF**
  - **Under evaluation for EAL4+**

Linux on System z

- **Common Criteria**
  - **SUSE LES9 certified at EAL3+ with CAPP**
- **Red Hat EL4 EAL4+ with CAPP and LSPP**

Virtualization

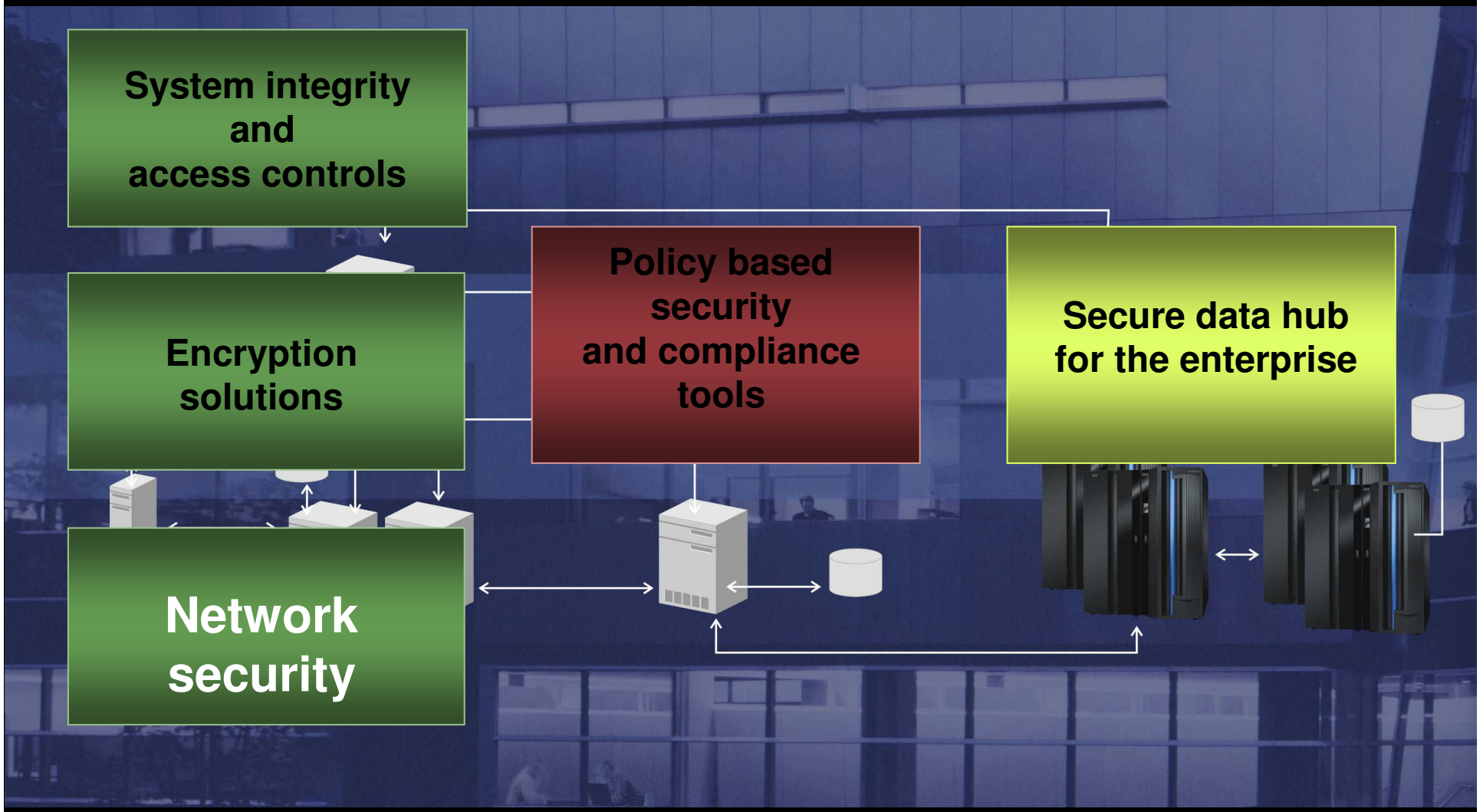
- Common Criteria EAL5 for Logical partitions

Cryptography

- **FIPS 140-2 level 4** for Crypto Express 2

www.**ibm.com**/security/standards/st_evaluations.shtml

Managing risk across the enterprise
System z Security Strategy

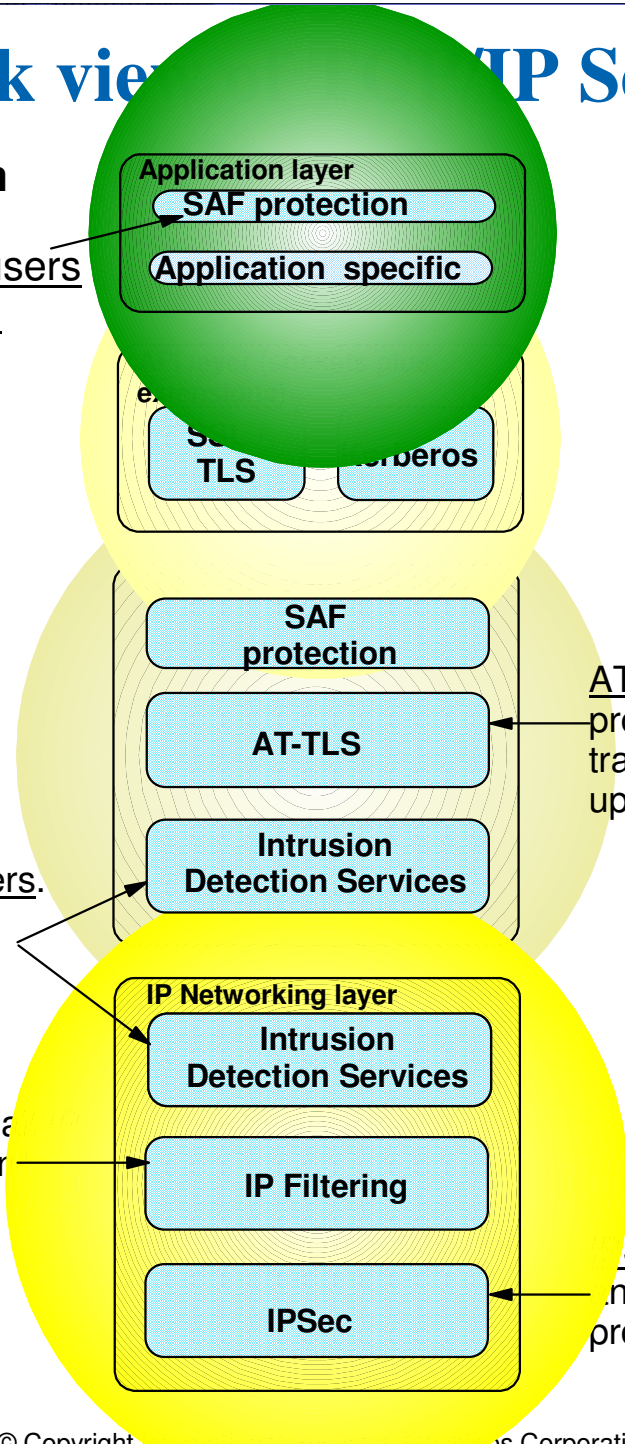


Protocol stack vie IP Security Functions

Protect the system

Use SAF to authenticate users and prevent unauthorized access

Protect data in the network



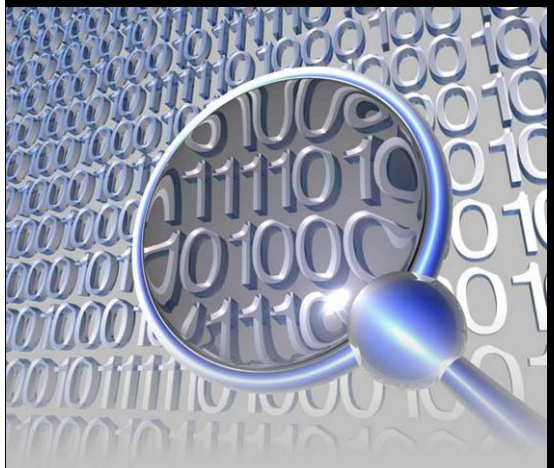
AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols.

IDS protection is provided at both the IP and transport layers.

IP packet filtering blocks out a traffic that this systems doesn specifically permit.

Sec resides at the networking layer nd is transparent to upper-layer protocols

Network security – z/OS Intrusion Detection Services



Detects events such as:
- Scans Attacks Flooding

Provides Defenses on z/OS
- Packet discard
- Limited # connections

Reports:
- Logging - Console
- Packet trace
- Notifications

A component of z/OS
Integrated in the IP stack

- Compliments network based IDS
- Enables further detection of attacks and application of defensive mechanisms
- Can be extended with Netview IDS

- Evaluates many known attacks
- Can evaluate unknown attacks
- Detects problems in real-time
- Policy based
- With z/OS 1.8, no longer requires LDAP

Helps protect against network attacks
Can evaluate IPsec inbound data after decryption

Network security – z/OS *encryption options over the Internet*

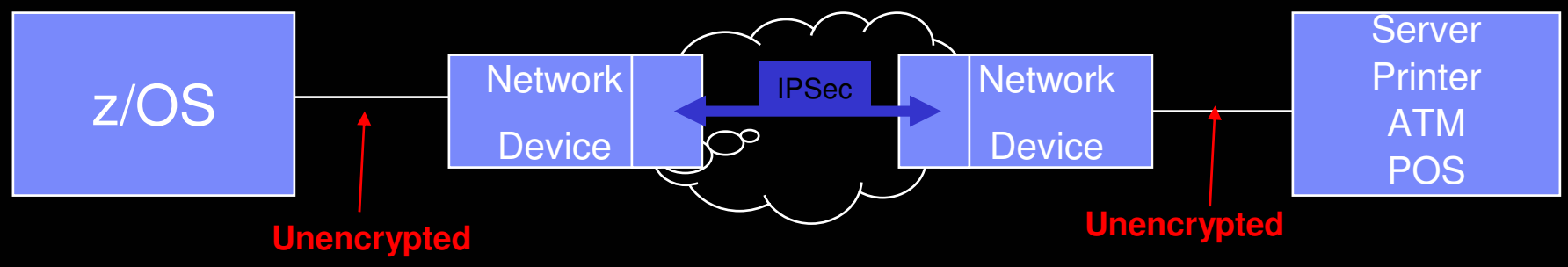
- **Application-based encryption**
  (with SSL and TLS)
  - **Encryption acceleration in the System z server**
- **End-to-end network encryption (with IPsec)**
  - Can create a secure tunnel for selected network traffic (Virtual Private Network)
  - **More compelling on System z with support for zIIP specialty processor**
- **File transmission encryption**
  - IPsec or SSL protected FTP, OpenSSH
  - Encryption Facility for z/OS

Simpler and consistent configuration with
Network Policy Agent in z/OS Communications Server

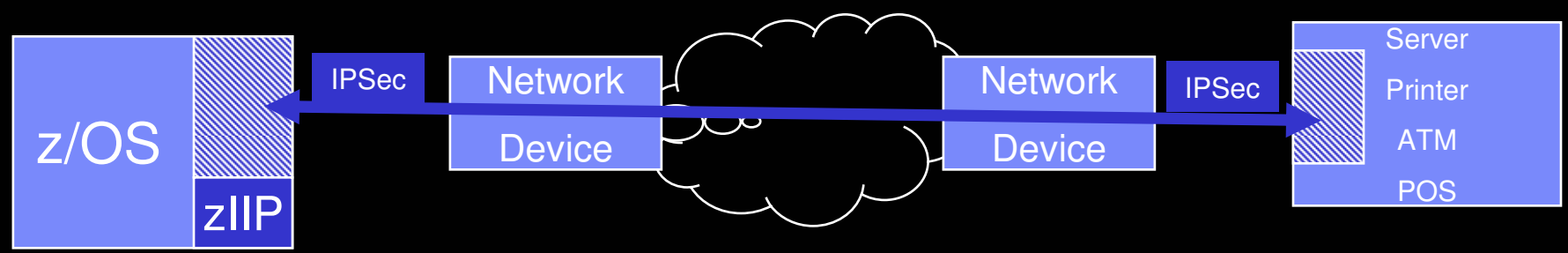
End-to-end network encryption

Growing requirement for companies that outsource some part of their network

zIIP specialty engine support helps reduce the cost of adding IPSec protection



Encryption in network devices



End-to-end encryption

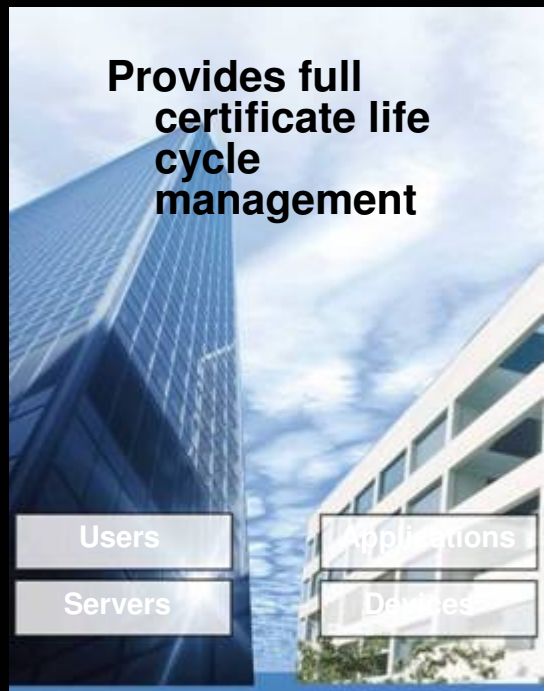
Digital Certificate hosting on System z

A digital certificate is an electronic "notary public" that establishes your credentials when doing business or other transactions on the Web.

A certificate authority (CA) is an authority in a network that issues and manages digital certificates.

z/OS PKI Services to enable a Certificate Authority solution

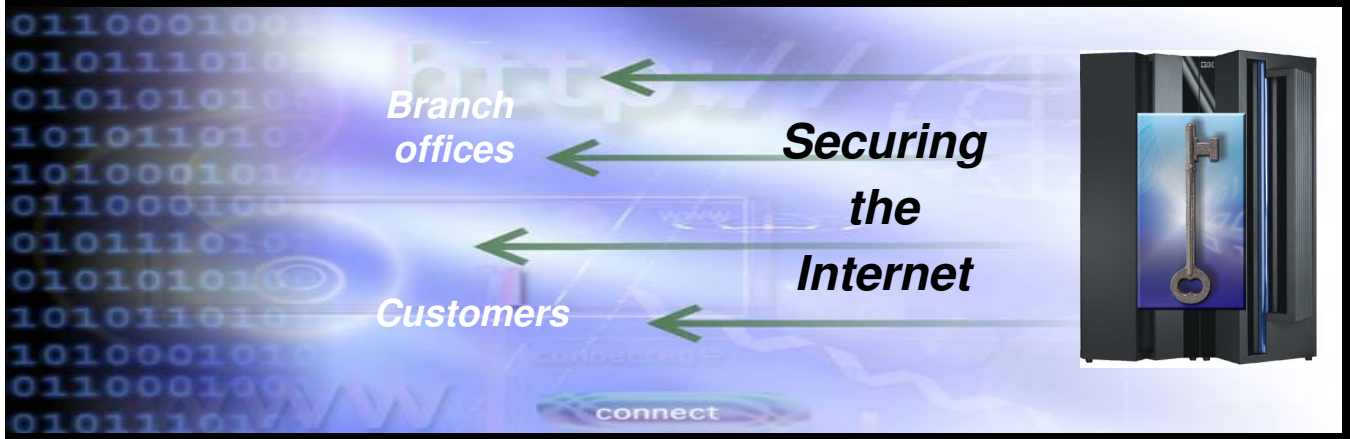
- TCO advantage - no need to pay a third party CA for certificates
- Relatively low mips to drive thousands of certificates
- Highly available (Sysplex exploitation)
- Secure with System z cryptography (Secure Key)



Used by large finance institution to avoid an estimated $16M a year

Banco do Brasil

- Saves an estimated $16 million a year in digital certificate costs
- Establishes a more secure enterprise network
  - by becoming their own Certificate Authority instead of paying third party
  - using the encryption solutions included in z/OS and their System z™ server

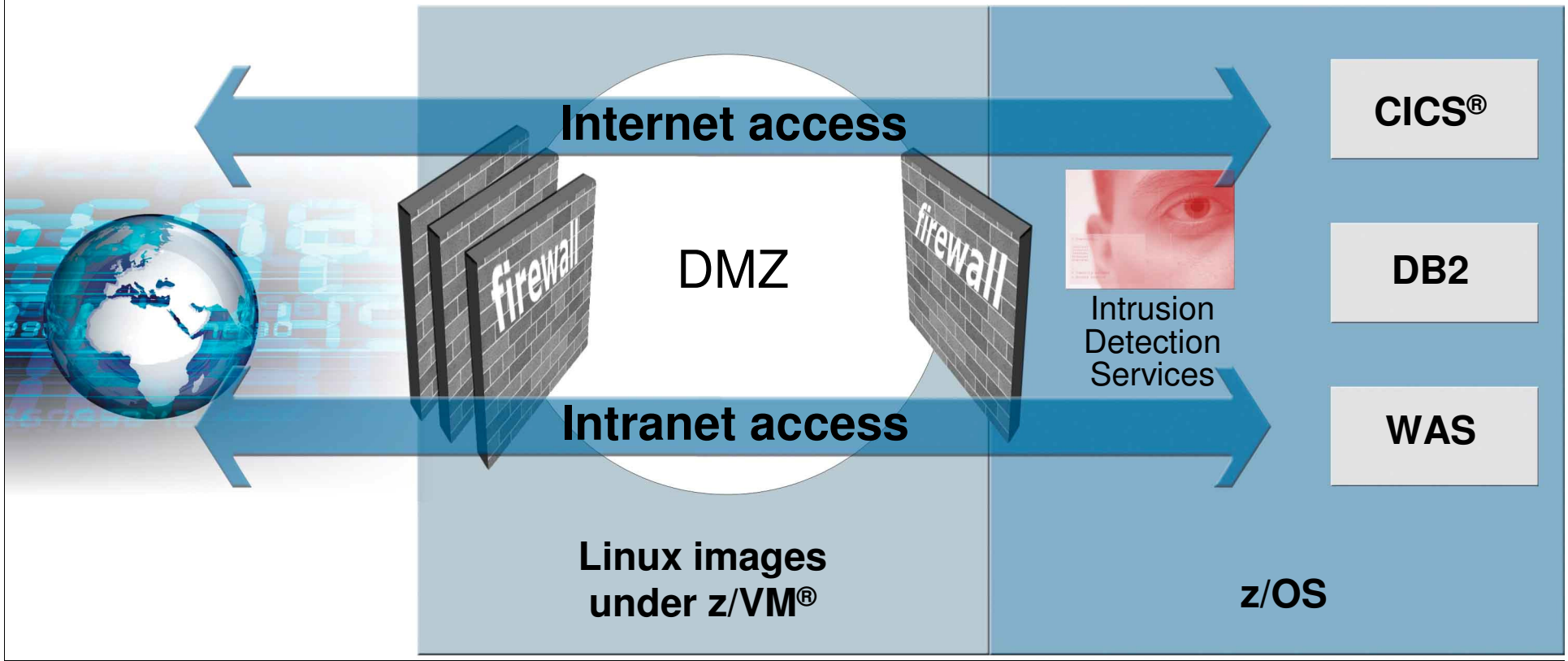


BANCO DO BRASIL

- 30 million accounts
- 4,000 locations
- 20 million transactions per day

Network security – perimeter defense
A DMZ on System z

- Leverage the integrity of mainframe virtualization
  - Logical Partitions with EAL5 certification and HiperSockets™
- *Stonegate*™ for centralized firewall policy management and firewall workload balancing

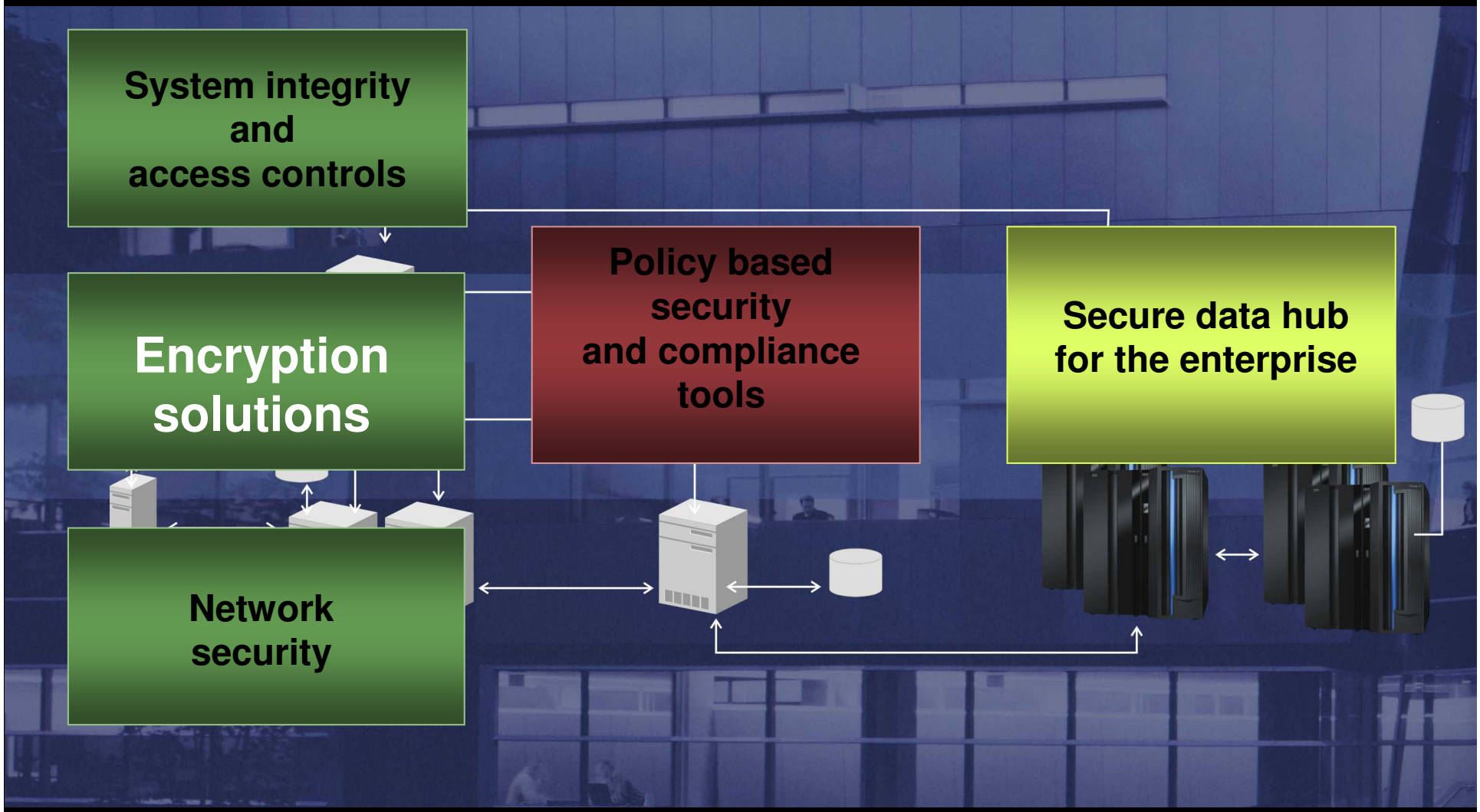


Defense in Depth

The threat prevention partnership of System z & ISS

- System z provides the industries' most securable platform
- ISS provides added network and application protection:
  - *Inbound traffic*
    - Can detect unwanted unencrypted traffic prior to its arrival at the mainframe
  - *Outbound traffic*
    - Can detect data leakage of unencrypted outbound data

Managing risk across the enterprise
System z Security Strategy



Mainframe Encryption Helping to Reduce Risk

Customer objectives:

- Only intended party is allowed to decrypt
- Availability of the keys and decryption services when you need them
- Protecting private keys by never exposing in the clear

Mainframe encryption options

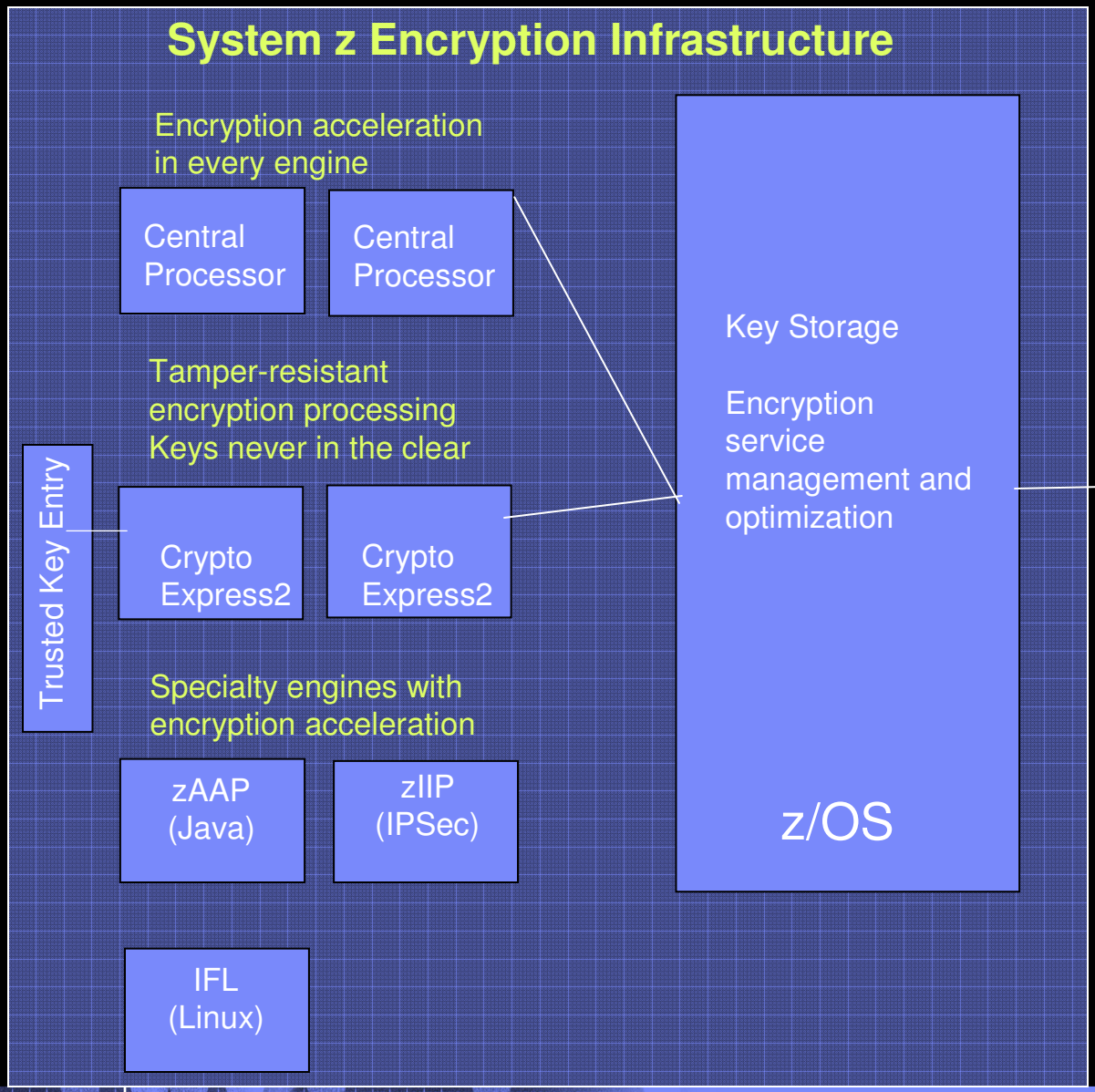
- Privacy over the Internet to customers and partners
- Highly secure transmissions to Printers, POS, ATMs, Network Devices, Servers
- Data in DB2® for z/OS®
- Data transferred on tape to business partners
- Archived data

Encryption acceleration

Secure-key processing

Centralized key management

System z Encryption Solutions



Encryption Solutions

- POS/ATM
- Internet Access
- Tape
- Future Disk Encryption*
- Database
- Web applications
- Application APIs PCKS#11, JEEC
- Digital Certificate Hosting
- "black box"

* IBM statement of direction

System z9 Cryptography Features

Methodology to help protect and manage keys

- Highly secure and available key data store
- Long term key management
- Disaster recovery capabilities
- Over 15 years of production use

Encryption acceleration

- Included in every System z9 general purpose engine
- Very high performance TDES, AES -128* and SHA-256*

For secure key processing

- "Tamper-resistant" packaging
- Important for highly secure encryption processing
  - ATM and POS support
  - Securing public and private keys
  - CVV validation, Trusted Key Entry,
- **Lower entry with single port card on z9 BC**
- **Linux on System z support**
- Holds Industry's top hardware rating - FIPS 140-2 Level 4

SSL acceleration

- Offloads compute-intensive RSA public & private-key cryptographic operations

*** Requires z9 EC or z9 BC**

Announcing the industry's first comprehensive end to end tape encryption solution

- IBM System Storage TS1120 Tape Drive
- Designed with a cross-IBM team driven by customer requirements
- New Encryption Key Manager program
- Integration with System z security and encryption capabilities
- Services and consulting

Customer Objectives
Data can only be decrypted by intended party
Keys available when and where you need them

TS1120 Tape Encryption – Key management basics

What keys are used?

- **Data encryption key -- used to encrypt (and decrypt) the data.**

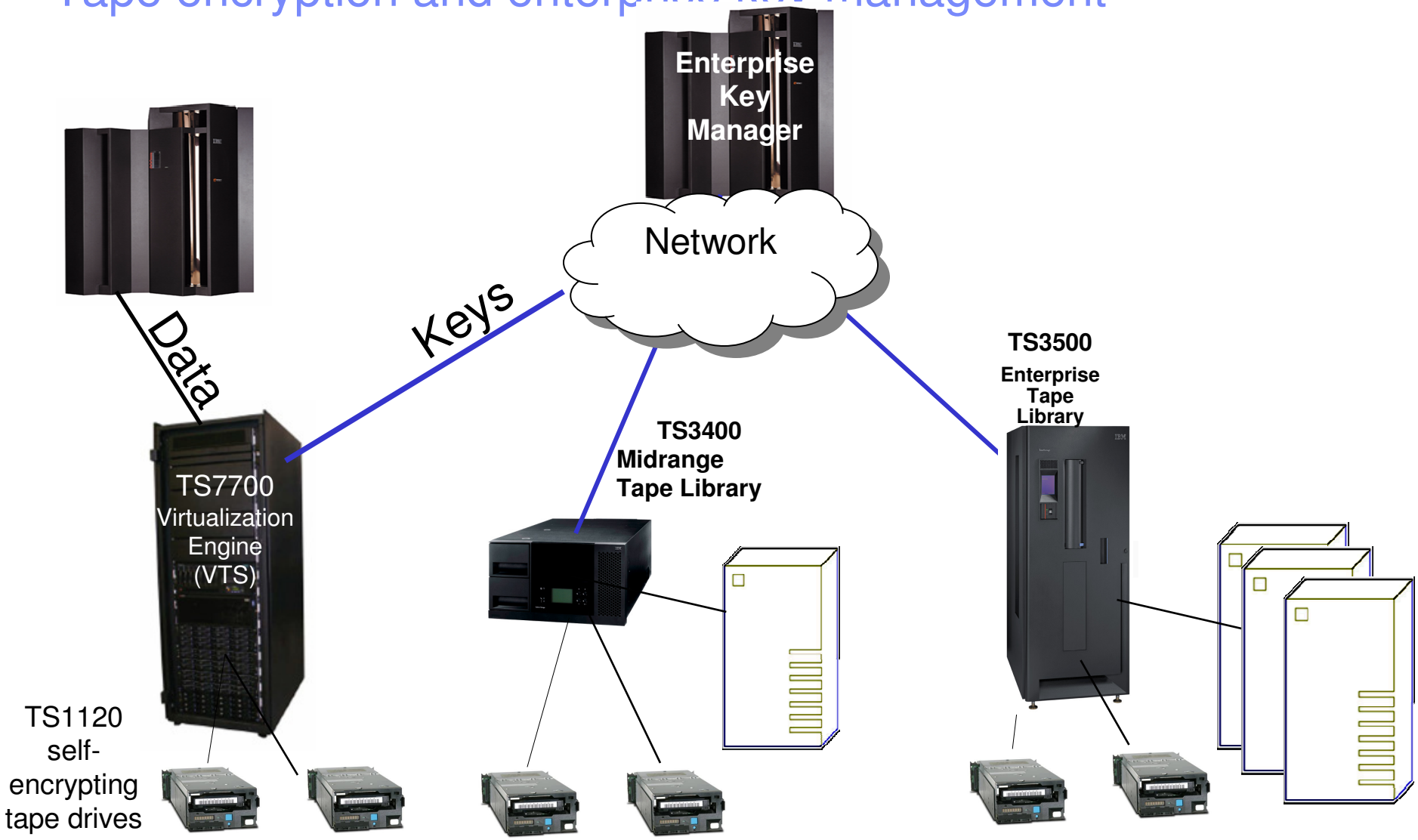
- **Public and Private keys - used to secure the data encryption key and allow only the authorized parties to decrypt.**
  - On System z these keys are processed using the tamper-resistant CryptoExpress2 module

Where are these keys stored?

- **The data encryption key is kept in the tape header, encrypted by the public key.**

- **The Public Keys (and Private Keys) are stored and managed by the host Enterprise Key Manager**
  - On System z the keys are protected under ICSF

Tape encryption and enterprise key management

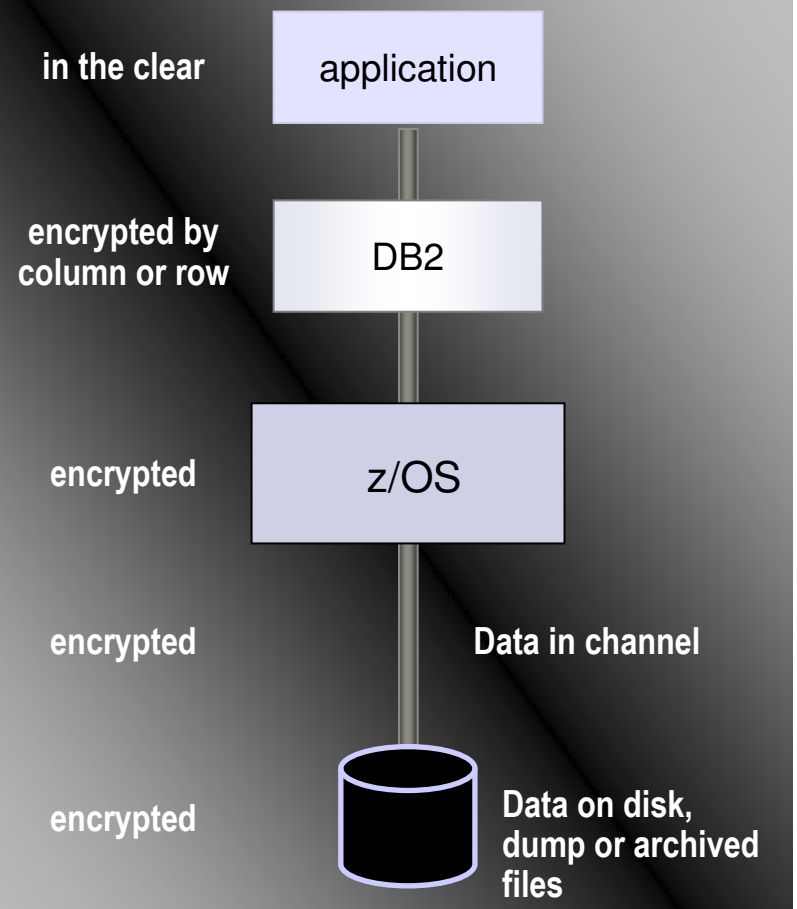


Protecting sensitive data with DB2 for z/OS

- **Encryption over the Internet**
  - **Encryption for DRDA® communications**
- **Encryption in the database**
  - **Column level encryption**
    - Enabled by the application itself
  - **Row level encryption**
    - IBM Encryption Tool for DB2 and IMS™

Using System z encryption acceleration and secure key processing

- **Mask sensitive data used in test environments**
  - DB2 Test Database Generator



System z Security

Mitigating the risk of security breaches

Helping to reduce the complexity and cost of enterprise security solutions

Robust security to enable consolidation

XXXXX says security breach will cost them

CNNMoney.com

Credit card fraud estimated by British Retail Consortium to have cost retailers 2.2 billion last year

NORWICH UNION
an AVIVA company

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

Agency Says Company Failed to Protect Sensitive Customer Data

- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Encryption solutions to help secure data from theft or compromise
- Highly secure network security
- Allowing you to address compliance needs with more confidence