La securite sur le system Z

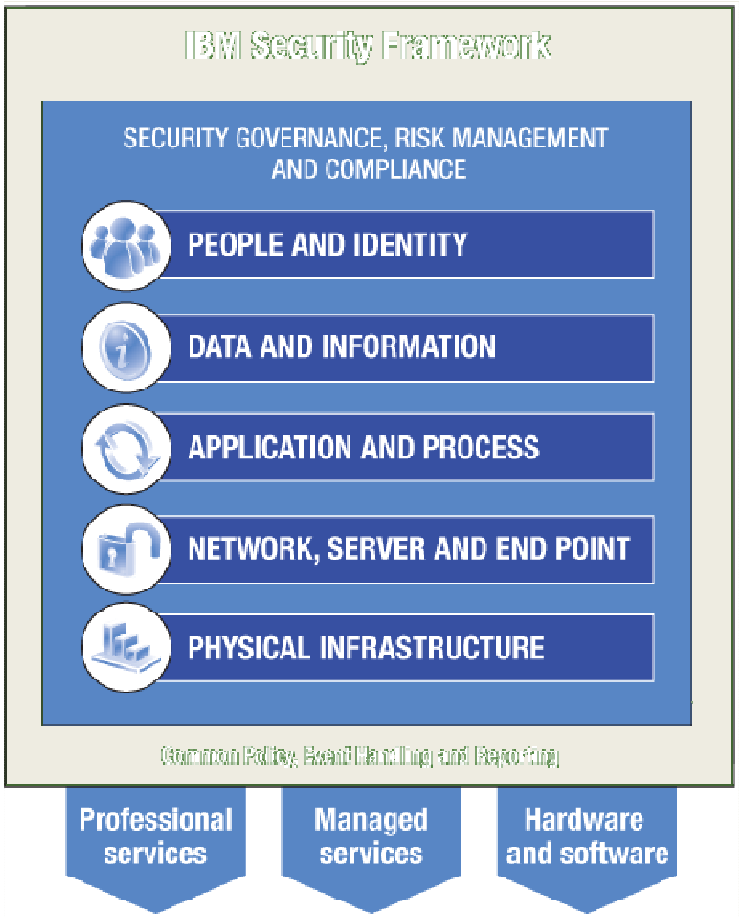
JM Darées

jmdarees@fr.ibm.com

Université du Mainframe 2013

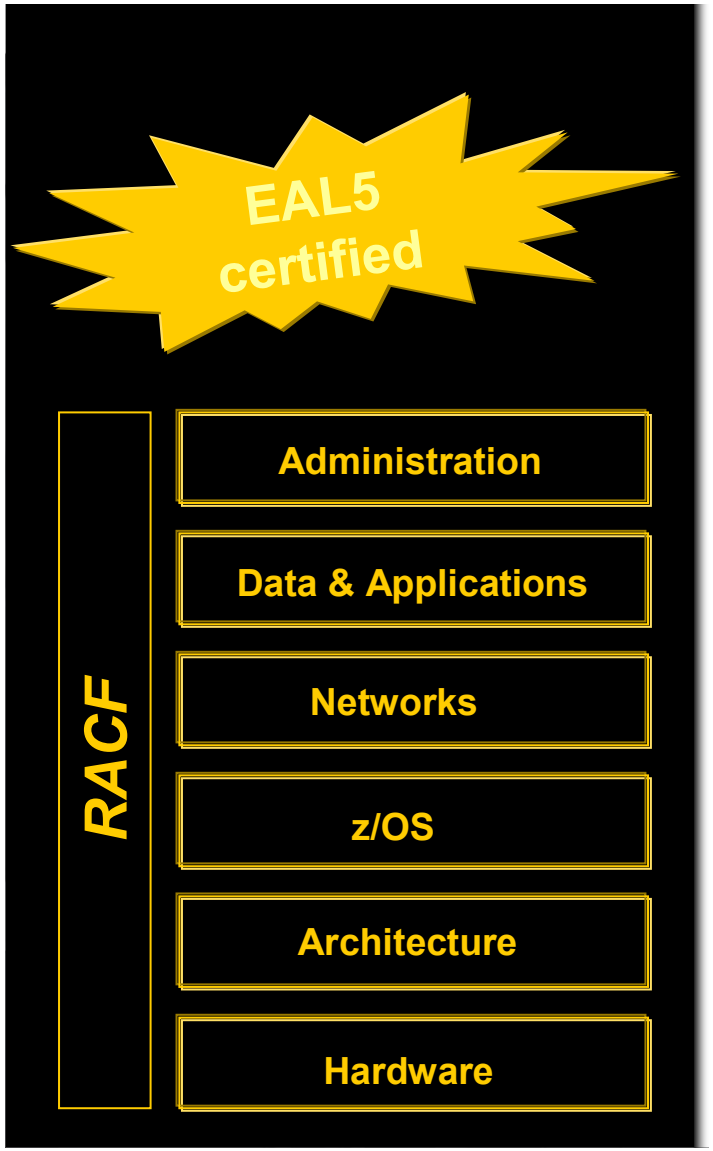
4-5 avril

IBM Security Framework



- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

Resource Access Control Facility (RACF)



- ✓ **Authentification**
- ✓ **Authorisation**
- ✓ **Administration**
- ✓ **Audit**

Resource Access Control Facility
RACF

Sécurise les application et les databases sans modification des applications

Réduit le cout et la complexité :

- Processus Centralisé Facile a appliquer aux nouveaux et a l' accroissements du nombre d'utilisateurs
- Suivi des activités qui permet d'adresser les besoin en terme audit et de conformité

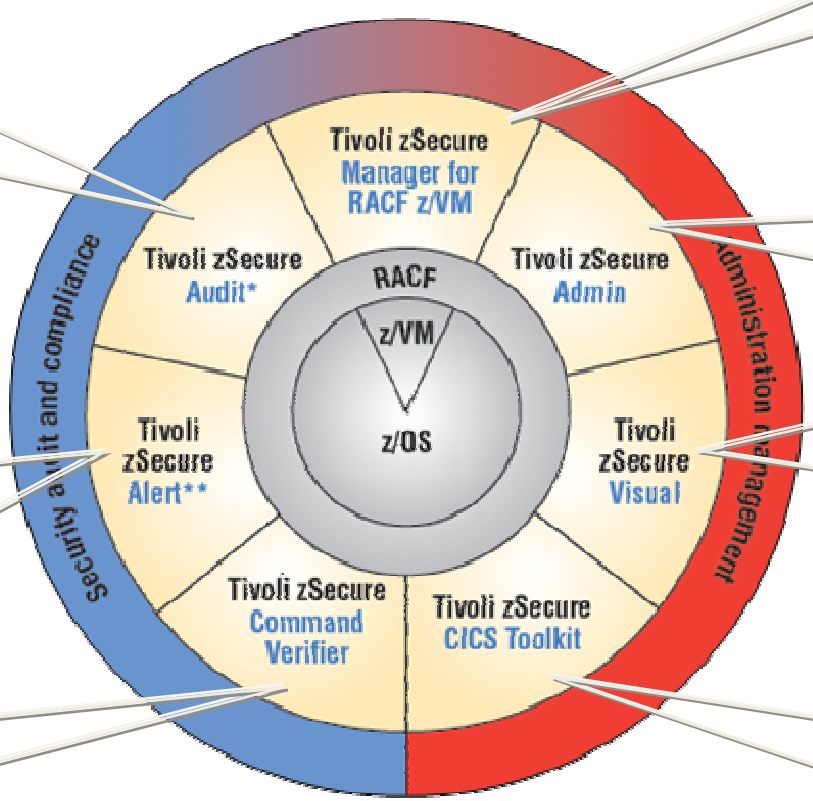
EAL5: https://www.bsi.bund.de/ContentBSI/EN/Topics/Certification/newcertificates.html

IBM Security zSecure

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands



Combined audit and administration for RACF in the VM environment

Enables more efficient and effective RACF administration, using significantly less resources

Reduces the need for scarce, RACF-trained expertise through **a Microsoft Windows–based GUI for RACF administration**

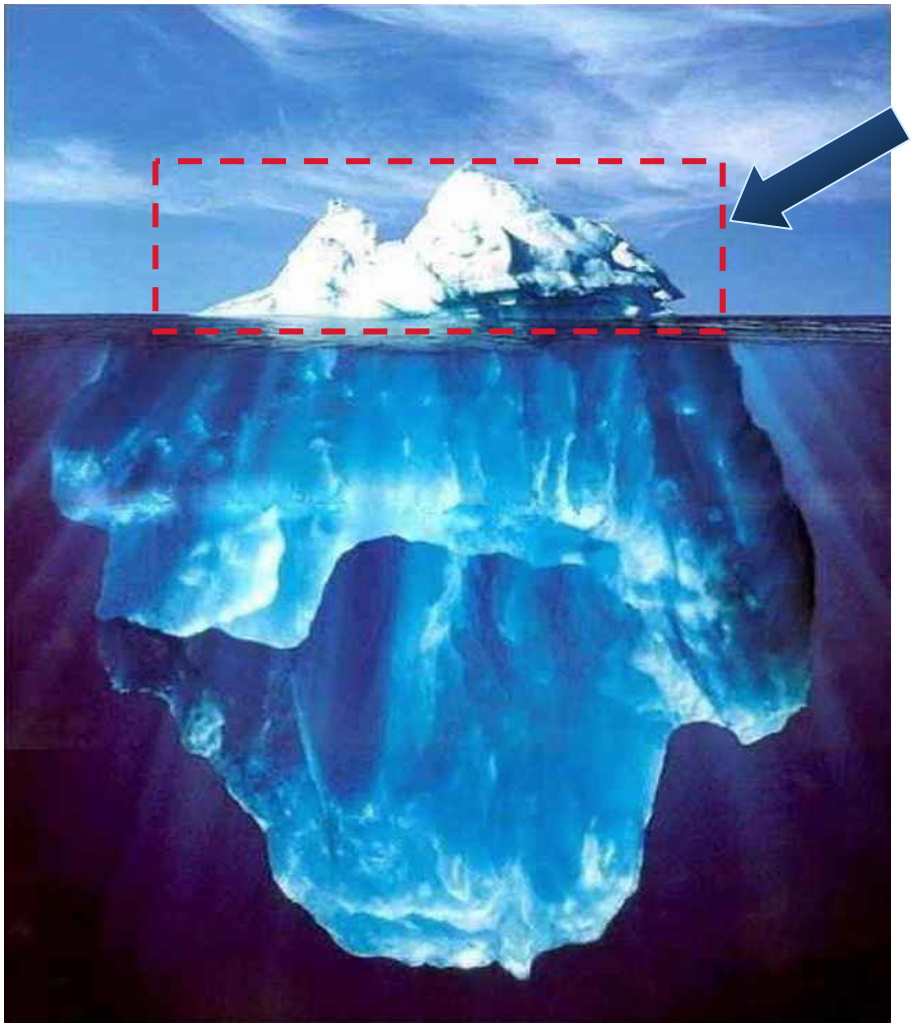
Allows you to perform **mainframe administrative tasks from a CICS environment**, freeing up native-RACF resources

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

z/OS PKI Services

- Un élément de base de Z/OS depuis plus de 10 ans.
- Il permet de réaliser toute les étapes du cycle de vie des certificats Digitaux
  - Requêtes utilisateurs via un interface web personnalisable
  - Browser ou serveur certificats
  - Processus d'approbation ou d'administration automatisable
  - Administré par la même une interface Web
  - Processus de révocation end user/administrateur
  - Déploiement de CRL (Certificate Revocation List) et de OCSP (Online Certificate Status Protocol)
  - Notifications par e-mail pour les requêtes de certificats et les alertes d'expiration.

IBM & Digital certificates



Une étude de la partie émergée de l' Iceberg seulement

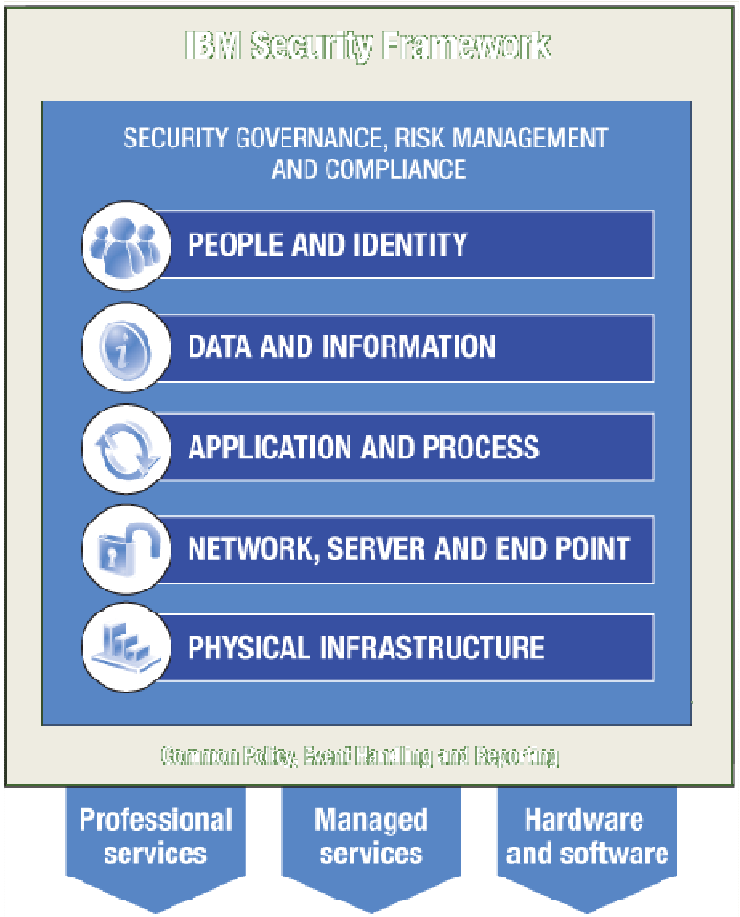
- Scan du port 443 (HTTPS) du réseau IBM
- Pas de scan derrière les firewalls de production
- Focalisé seulement sur les server certificats existants.

Résultats:

- 60,000 certificats découverts
- 6,000 certificat a $500); Economies potentielle estimée: **3 millions $**


IBM
Hello, Jonathan M. Barney | Log Out
IBM Certificate Authority - Personal Certificate
w3 Home | BluePages | HelpNow | Feedback
My Certificates | Manage | Help
Personal Certificate
Key Generation
$3M savings
Deliver certificates to all IBMERs using:
Submit
Cancel
Terms of use | Issue Tracking
Autoridade Certificadora Interm
PKI Services - GERAÇÃO DE CERTIFICA
Escolha uma opção:
Solicitar Certificado
Receber Certificado
$16M savings
BANCO DO BRASIL

IBM Security Framework



- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

Guardium DB2, IMS Data Encryption on System z

Protecting sensitive and confidential data

IMS Segment Edit/Compression exits

- DECENC01 – Secure key
- DECENB01 – CPACF Protected key

DB2 EDITPROCs

- DECENC00 – Secure key
- DECENA00 – Clear key
- DECENB00 – CPACF Protected key

Specified in the EDITPROC clause of the SQL CREATE TABLE statement.

One different key per table if desired.

Indexes not encrypted.

Row level encryption.

No application changes.

DB2 FIELDPROC

- DECENF00 – CPACF Protected key

Indexes encrypted.

Column level encryption.

No application changes.

DB2 User Defined Function (UDF)

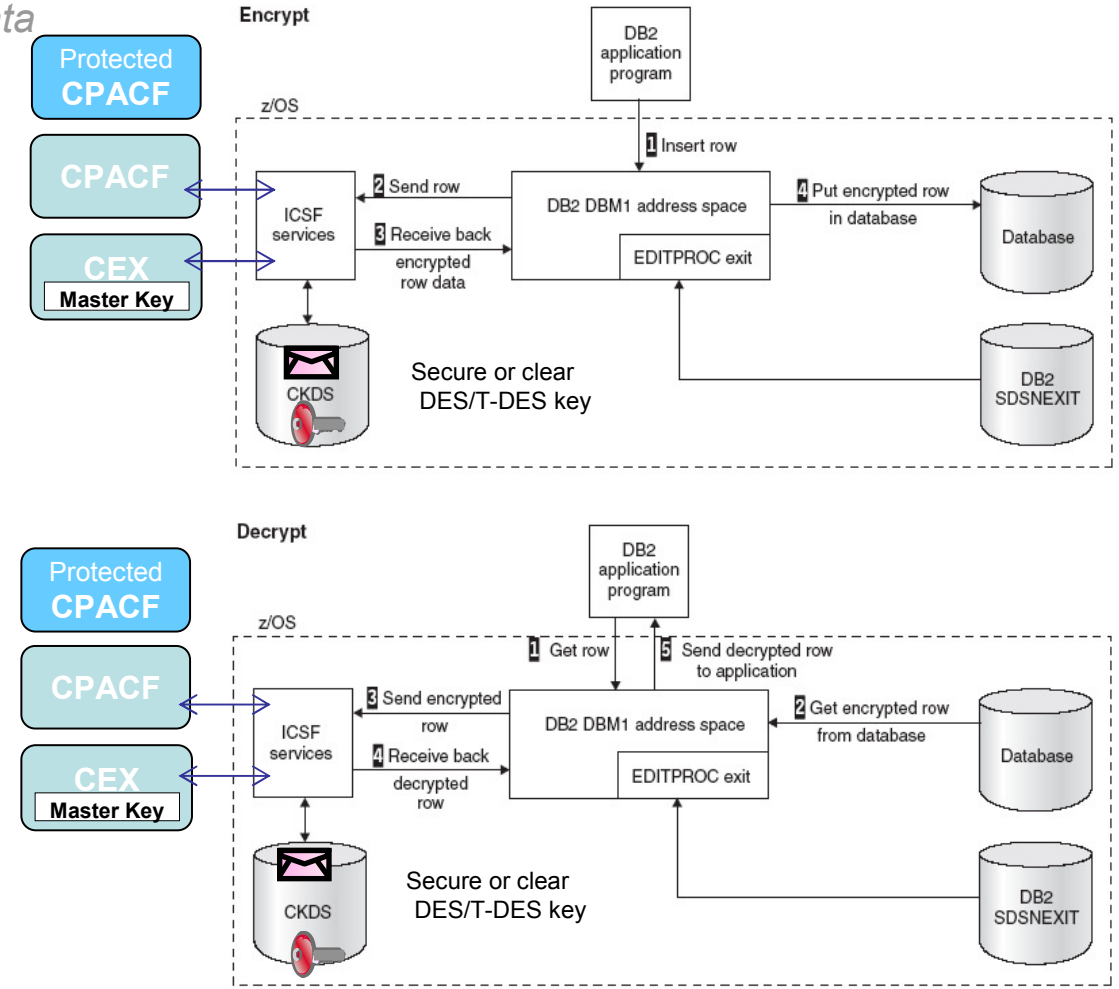
- DECENU00 – CPACF Protected key

Indexes encrypted.

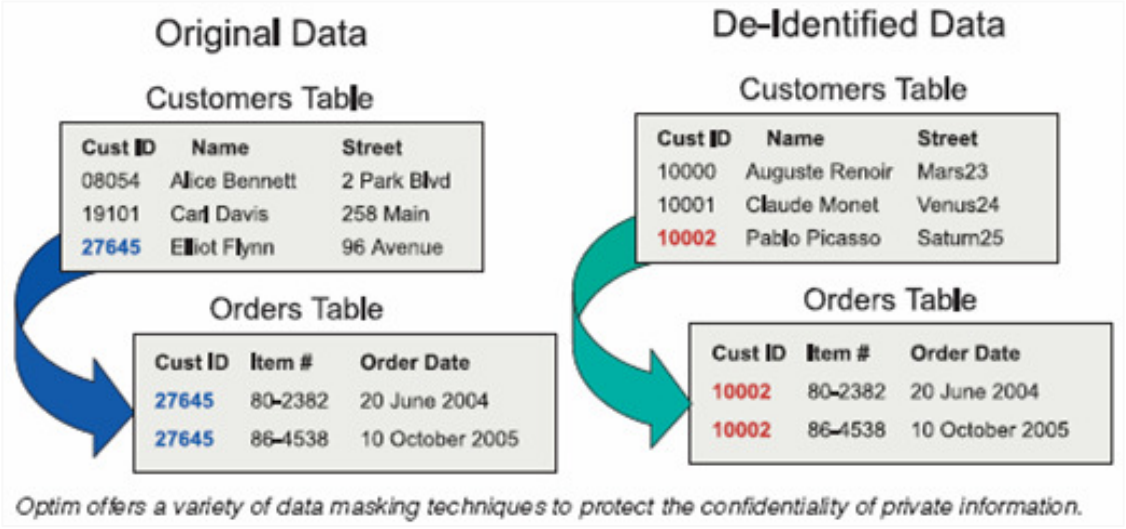
Column level encryption.

Application changes, but better access control when used with VIEW, TRIGGER and MASK SQL statements..

Note: impacted data is encrypted in the DB2 buffer pool.



Infosphere Optim



Production

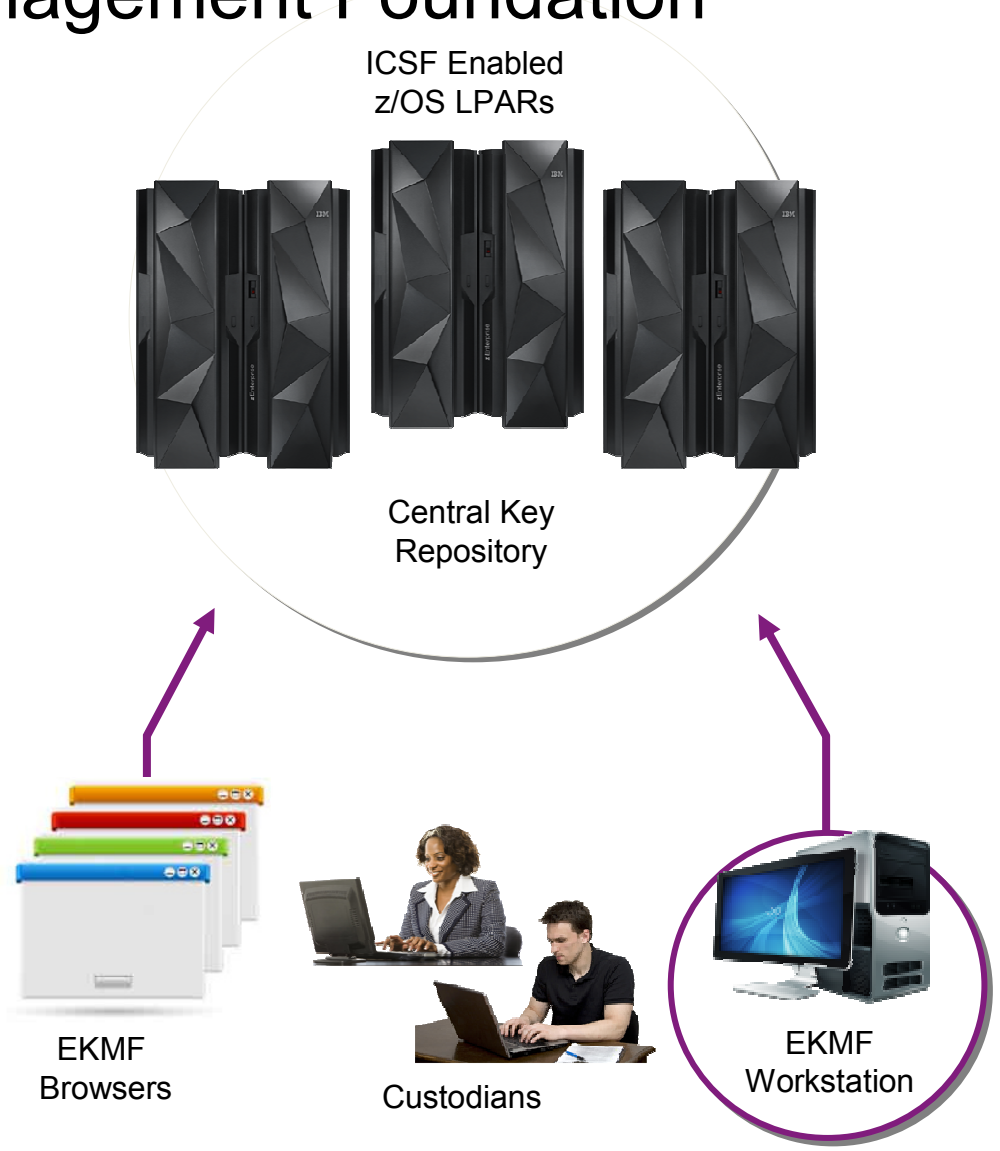
↓

Test/Dev

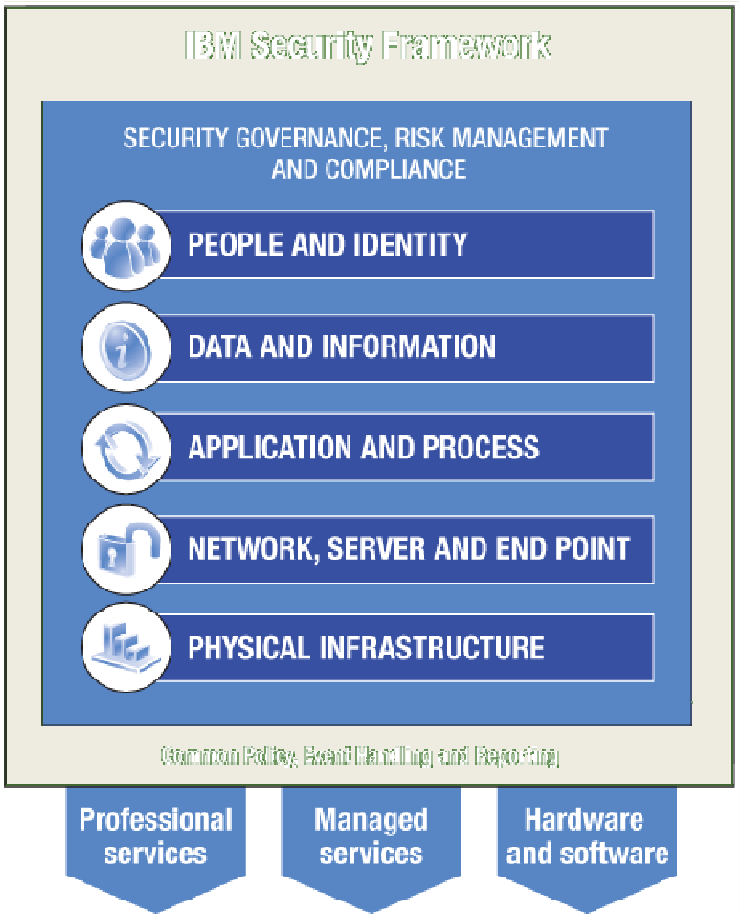
IBM Enterprise Key Management Foundation

- IBM EKMF est composée d'une workstation hautement sécurisée, des application browsers et un répertoire central.
- Toutes les nouvelles clefs sont générées sur la workstation . Elle est sécurisée par une authentification forte via smart cards. L'EKMF Workstation embarque une IBM 4765.
- Les fonction du EKMF browser propose des solutions de monitoring et permet l'automatisation d'opération sur les clefs..
- Le répertoire de clefs contient des clefs et des meta data. Il permet des solutions de Backup/restore efficientes .

Note that while this is a mainframe centric view, EKMF supports distributed platforms as well

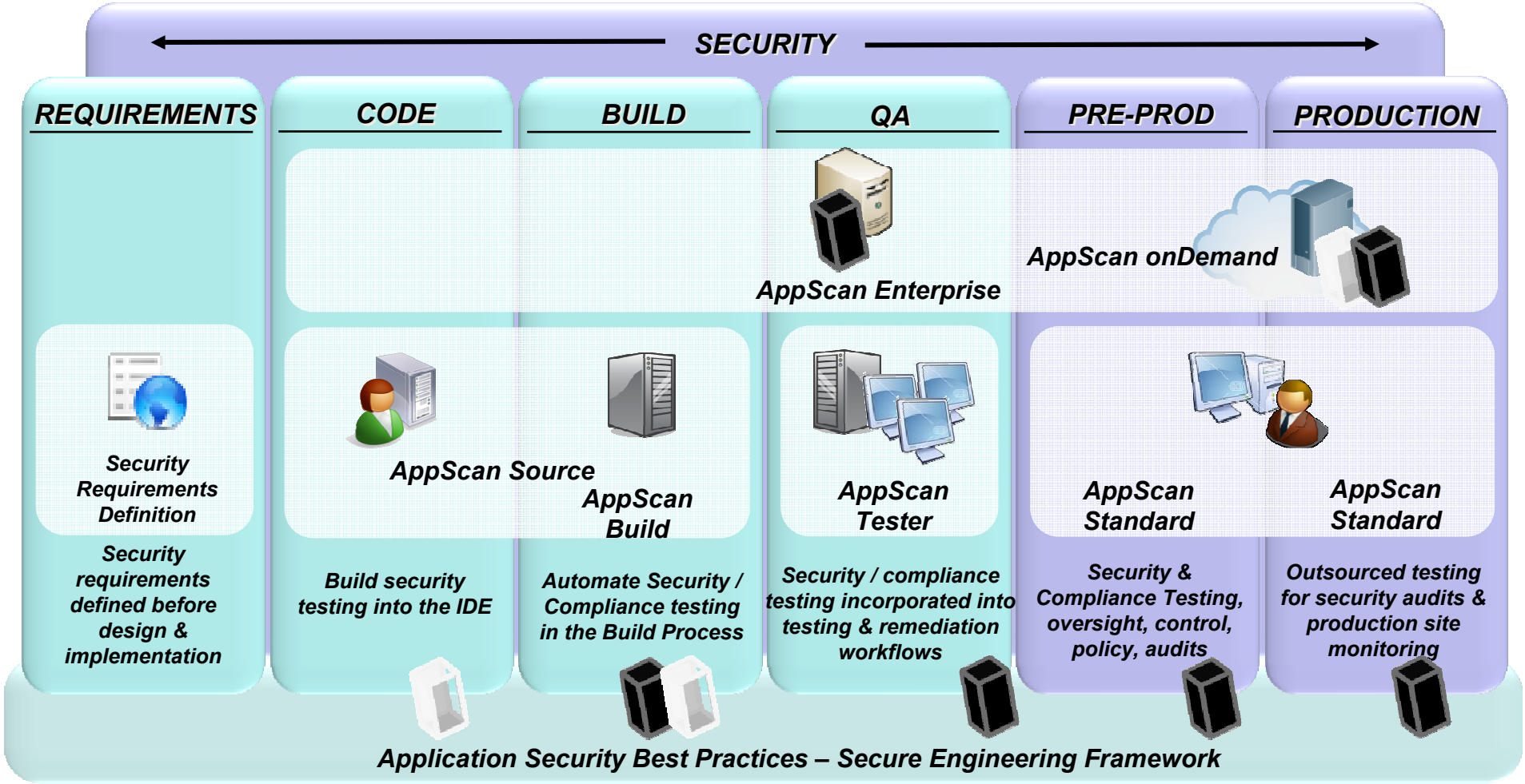


IBM Security Framework



- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

IBM Rational AppScan Suite

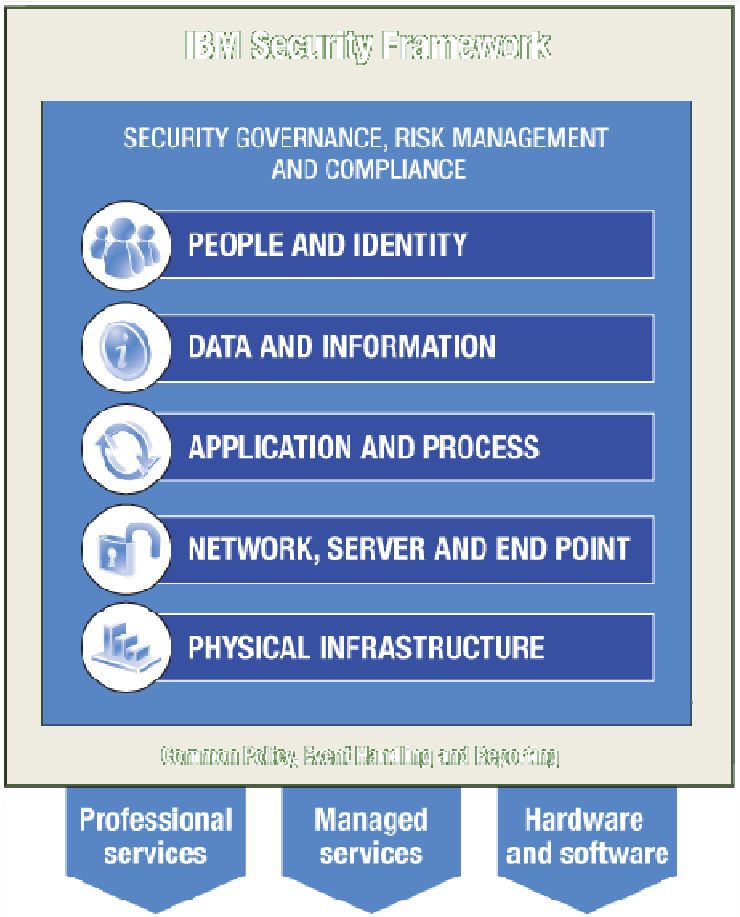


Execute what you trust !!!

Code signing

- Code signing pour les Program Objects (PDSEs)
- Supporte Program Management Binder & Loader
- System SSL supporte un mode of operation conçu pour atteindre le NIST **FIPS 140-2** Level 1
- AT-TLS support for FIPS 140-2

IBM Security Framework

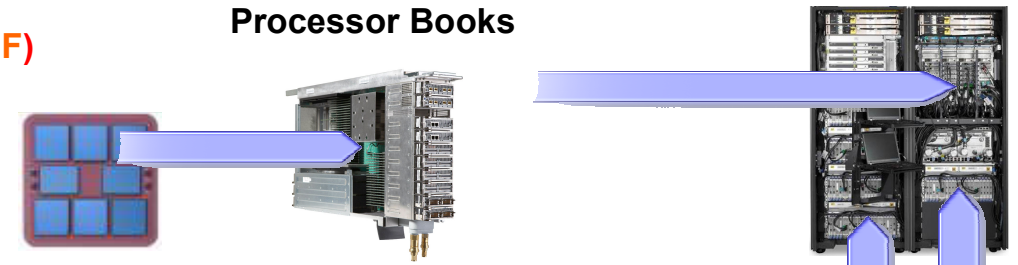


- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

System z Hardware Cryptography Implementation

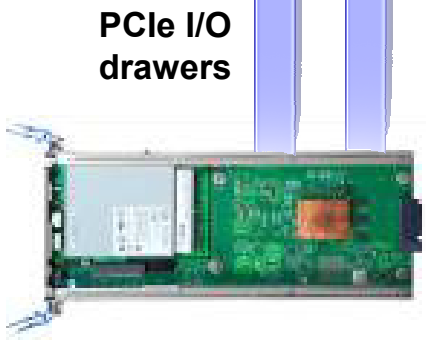
CP Assist for Cryptographic Functions (CPACF)

- A facility integrated in each PU
- Standard orderable feature
- Clear Key & Protected Key only
- Symmetric, hash, …



Crypto Express 4S (CEX4S)

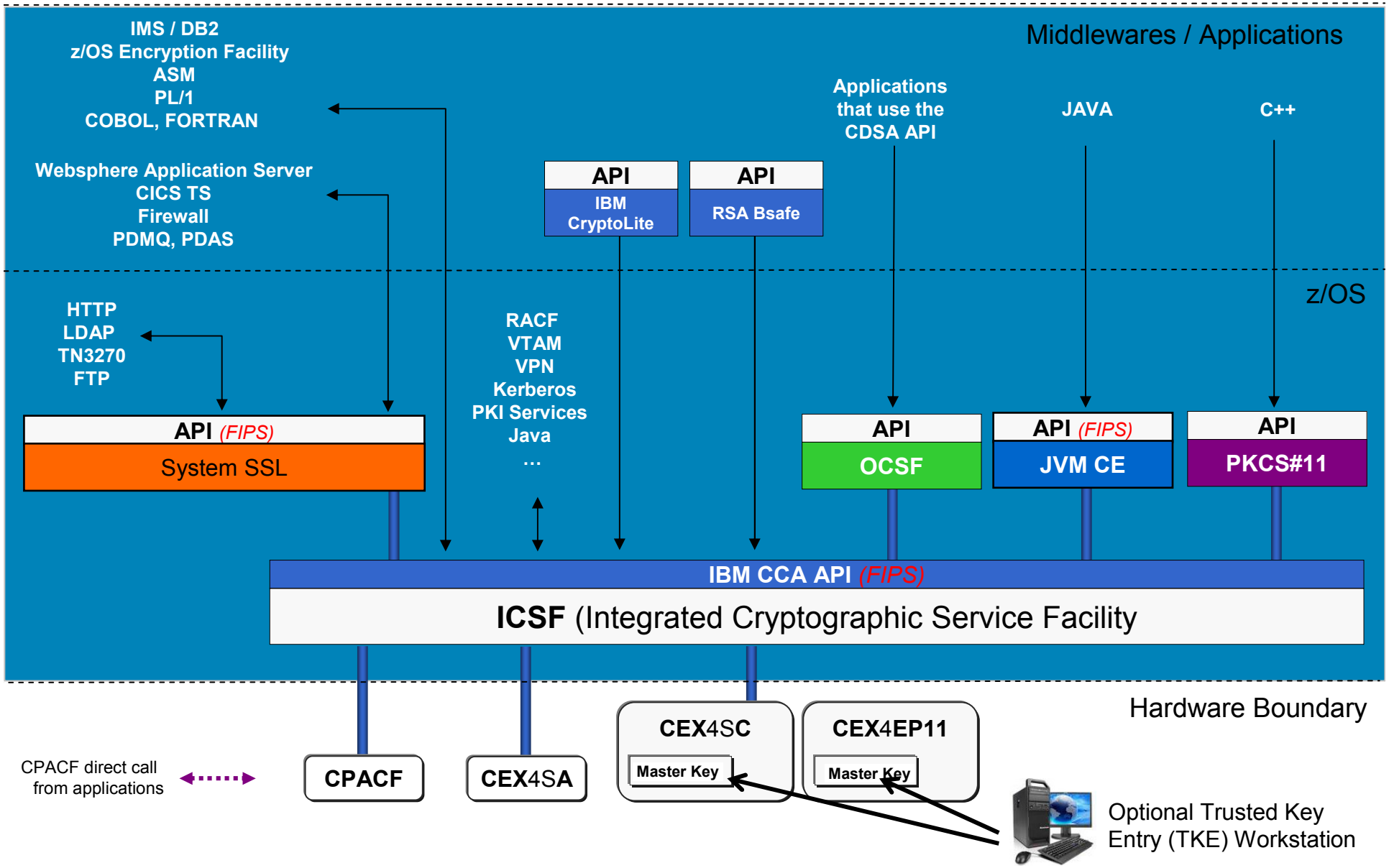
- Priced feature
- 0-16 features in a system
- 1 secure **4765 coprocessors** per feature
- Secure key symmetric (DES, T-DES) and asymmetric (RSA)
- PR/SM sharable
- Manually configurable into an RSA accelerator (CEX3A)
- **FIPS140-2** Certified (As Coprocessor only)



configuration options

Accelerator	CCA Coprocessor	EP11 Coprocessor
FIPS140-2 = NO	*FIPS140-2 = YES*	*FIPS140-2 = YES* *EAL5+ = YES* *QDS Certified = YES*

Crypto Infrastructure – z/OS R13



Exploitation de la Crypto Hardware

Protect Data in transit

Protect privacy of customer & employee information

Encryption with key management

Highly secure data transfer

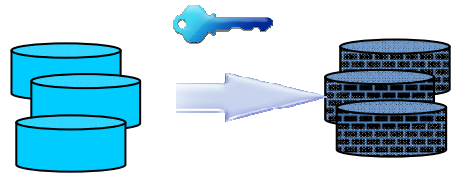
Information Integrity

Ensure integrity of information, SoD for encryption of data at rest

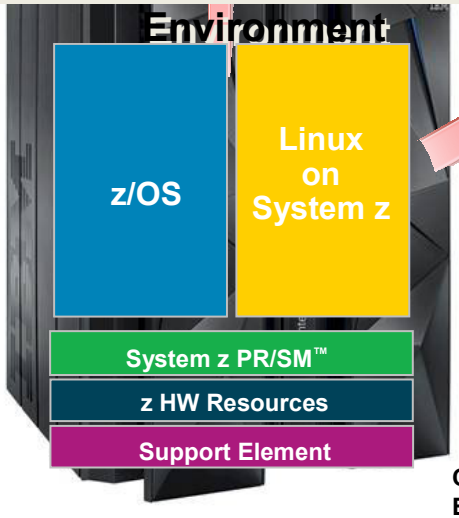
Encryption of data for archival

Encryption

z/OS key management capabilities
Long term key management



The Secured Business Environment



Crypto Express

Protect your Communications

Enabling non z/OS servers to communicate securely with z/OS.

FTP, FTPs
OpenSSL, OpenSSH

IPsec

Secure exchange of business critical information

Highly secure transfers across the Internet

Trusted exchange with open standards & support for **IP encryption**

Digital Certificates

Trusted business transactions

PKI and Digital Certificates

Identrus compliant Certificates

Directory Services

Managing identity across enterprise

Security Administration

Data Security

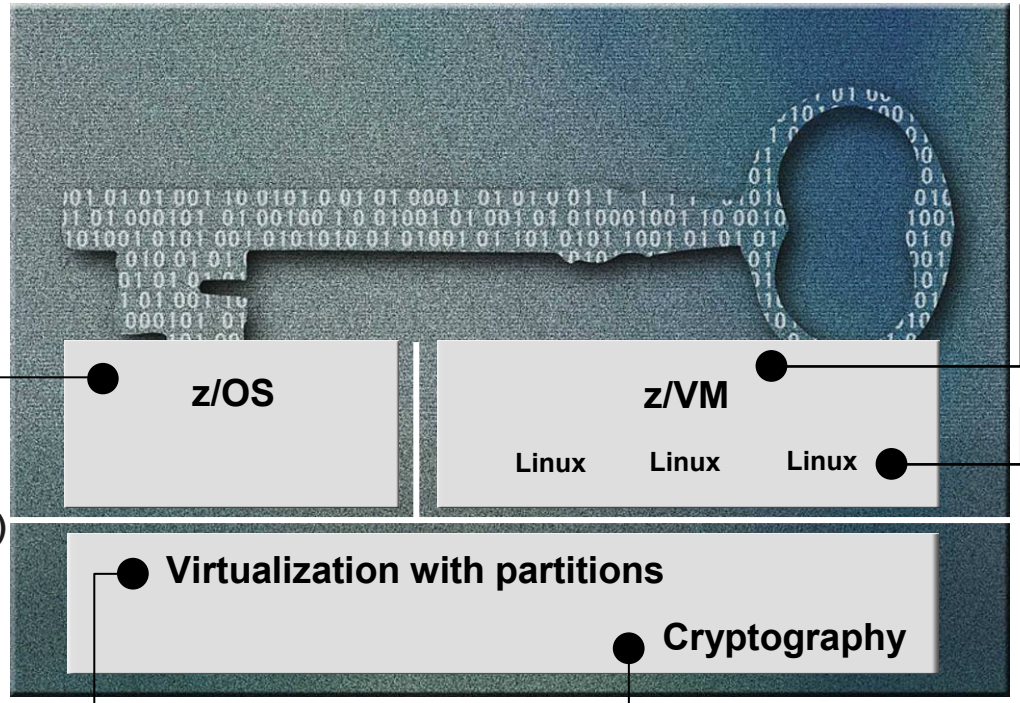
Single repository of data with various levels of security

Distributed directory services

Certifications

Certification of mainframe products and components

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- Common Criteria EAL4+
  - with CAPP and LSPP
  - z/OS 1.12 RACF (OSPP)
  - z/OS 1.13 under evaluation
- IdenTrust™ certification for z/OS as a Digital Certificate Authority (PKI Services)
- System Integrity Statement

z/VM

- Common Criteria
  - z/VM 5.3
  - EAL 4+ for CAPP/LSPP
  - System Integrity Statement
  - Plan to have z/VM 6.1 evaluated during 2011

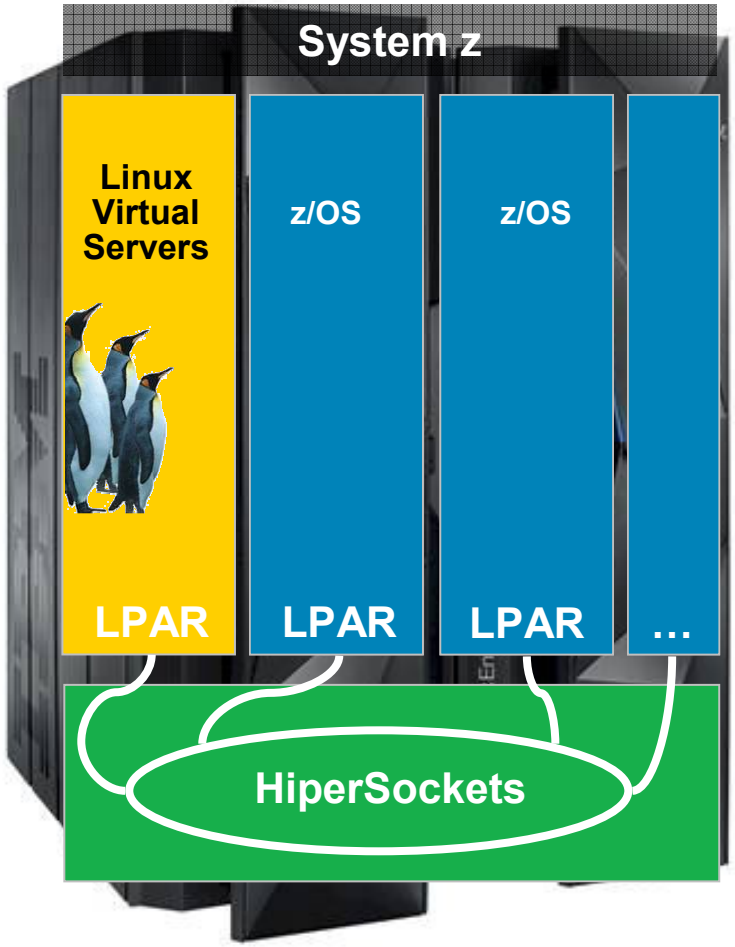
Linux on System z

- Common Criteria
  - SUSE LES10 certified at EAL4+ with CAPP
  - Red Hat EL5 EAL4+ with CAPP and LSPP

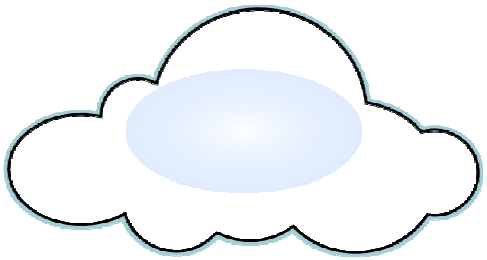
- Common Criteria EAL5+ for Logical partitions
- FIPS 140-2 level 4 for Crypto Express 3

See: www.ibm.com/security/standards/st_evaluations.shtml

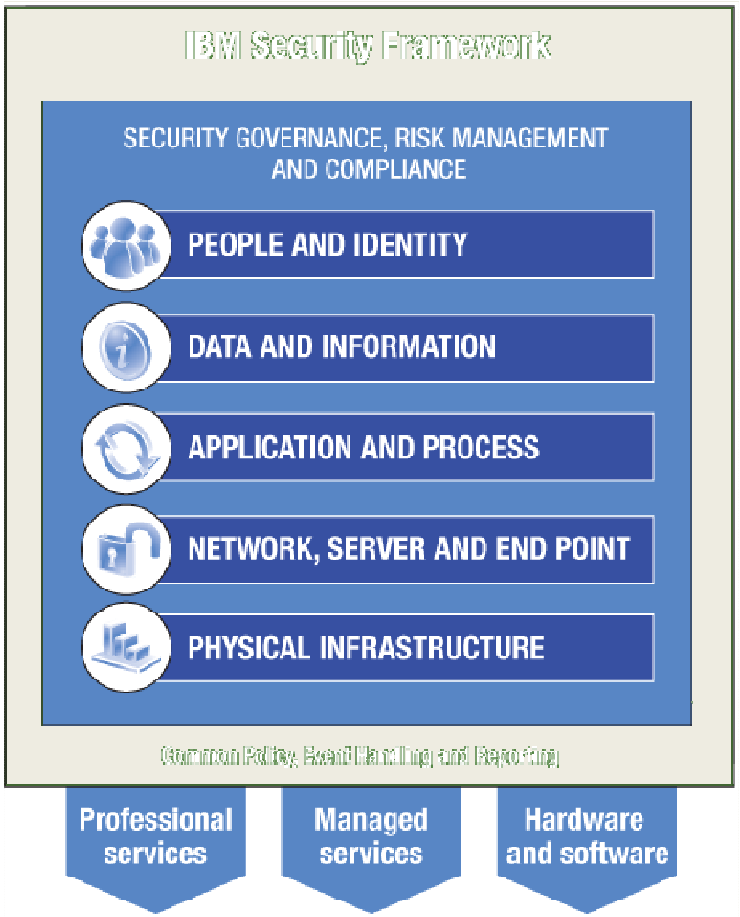
Cloud Secure et Virtualisation



- **Virtual servers on a single mainframe: Logical Partitions (LPAR)**
  - Plus haut niveau de « Common Criteria certification for server virtualization » – **EAL5**
- **Virtual network : HiperSockets**
  - Propose un TCP/IP Base sur de la mémoire système
  - Permet de mettre en place un "Data Center" inside a box " compose d' images z/OS et Linux
  - Connexion hautement secure – pas de réseau externe

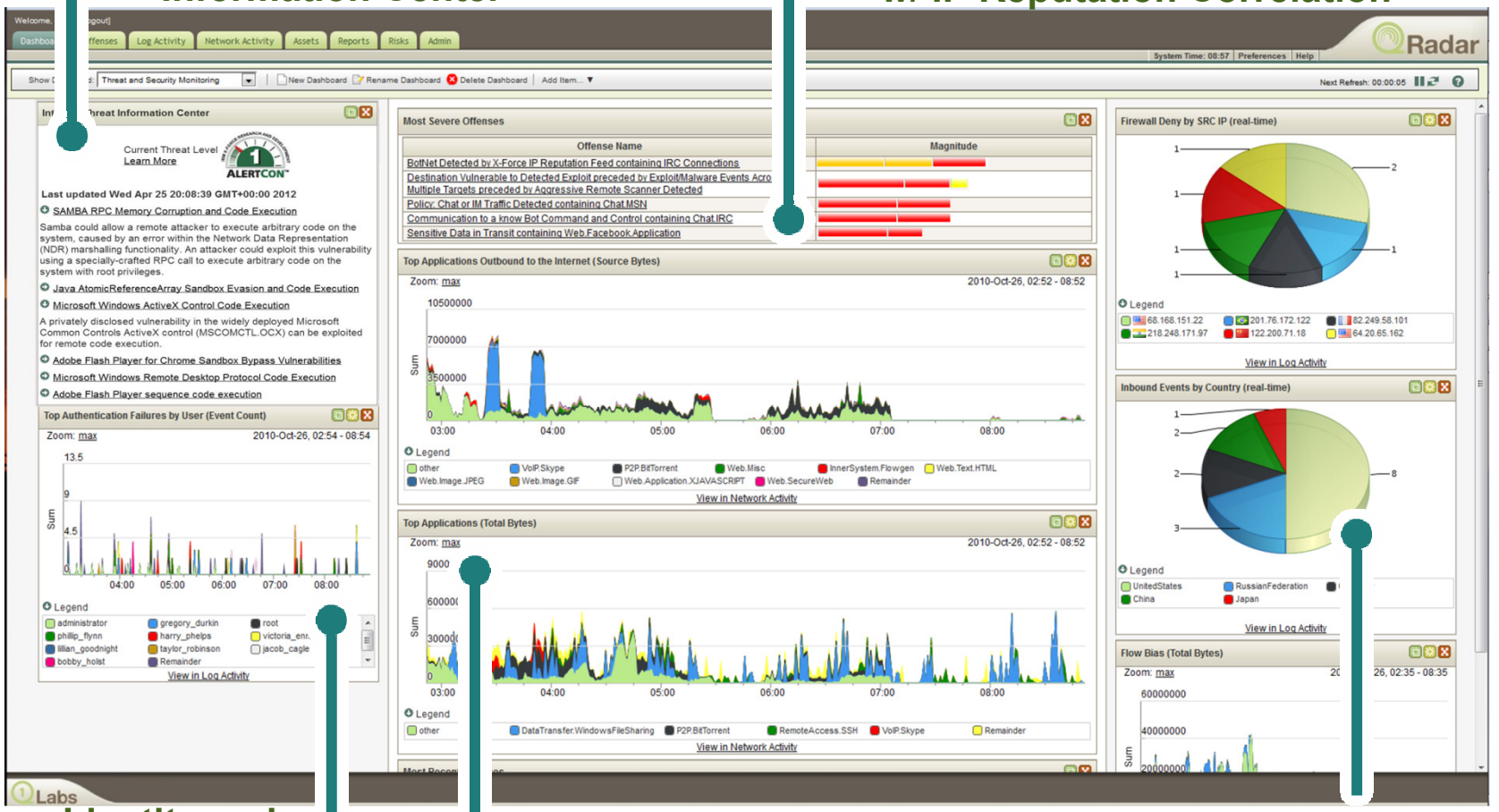


IBM Security Framework



- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

Security Intelligence: *QRadar*



PCI & System z

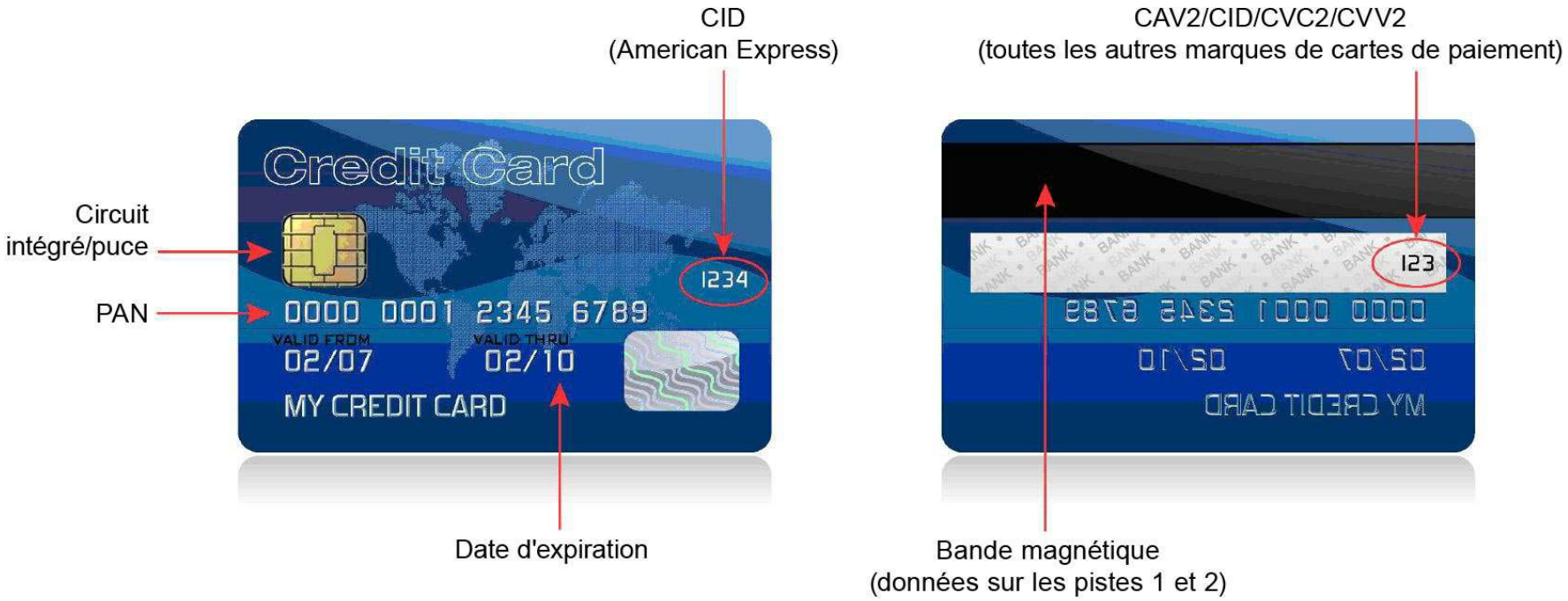
PCI Payment Card Industry Data Security Standard.

Les données de la carte bancaire sont devenues sensibles car elle permettent de faire un paiement sur internet sans présence physique de la carte. Les fraudeurs cherchent à capturer ces numéros en attaquant les systèmes d'information des acteurs qui stockent ces données. Le programme PCI DSS vise à améliorer la sécurité physique et logique des systèmes d'information en demandant aux acteurs de respecter des bonnes pratiques de sécurité.

A qui s’applique la norme ?

- PCI DSS s’adresse à tous les acteurs qui capturent, transportent, stockent et/ou traitent des données de cartes bancaires. Les commerçants de proximité, les marchands sur internet, les réseaux de transport, les centres d’appels, les banques, les émetteurs de cartes font partie des acteurs concernés par PCI DSS..

Les données a protéger



Directives relatives à la norme PCI DSS

- **Création et gestion d'un réseau sécurisé**
  - Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes
  - Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le

  fournisseur
- **Protection des données des titulaires de cartes de crédit**
  - Condition 3 : Protéger les données de titulaires de cartes stockées
  - Condition 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
- **Gestion d'un programme de gestion des vulnérabilités**
  - Condition 5 : Utiliser des logiciels ou des programmes antivirus et les mettre à jour régulièrement
  - Condition 6 : Développer et gérer des systèmes et des applications sécurisés
- **Mise en œuvre de mesures de contrôle d'accès strictes**
  - Condition 7 : Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître
  - Condition 8 : Affecter un ID unique à chaque utilisateur d'ordinateur
  - Condition 9 : Restreindre l'accès physique aux données des titulaires de cartes
- **Surveillance et test réguliers des réseaux**
  - Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes
  - Condition 11 : Tester régulièrement les processus et les systèmes de sécurité
- **Gestion d'une politique de sécurité des informations**
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel

Un changement profond pas toujours compris

PCI n'est pas seulement un **datacenter certifié PCI DSS** avec l'installation de quelques logiciels de sécurité PCI

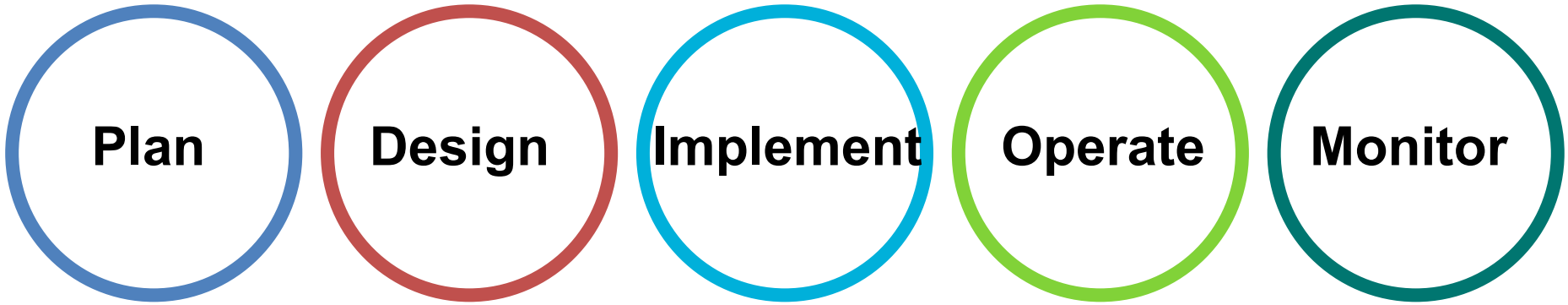
C'est :Une conformité pluri-disciplinaire

- un datacenter certifié PCI DSS
- des contraintes d'implémentations techniques
- des logiciels de sécurité
- ….

Mais surtout la mise en place des **processus organisationnels**, la rédaction de documentati précise et l'audit régulier des systèmes.

Services Professionnels PCI DSS d'IBM

Les Services Professionnels PCI DSS d'IBM permettent aux entreprises d'établir un environnement de confiance pour gérer l'ensemble exigences PCI DSS de bout en bout, et ainsi d'atténuer les risques de fraudes.



Plan

Identification des enjeux métier et des objectifs de sécurité

Définition et réduction du périmètre PCI DSS

Développement d'une stratégie

Évaluation de l'état actuel, analyse des écarts

Design

Définition des politiques et des procédures PCI DSS

Définition des rôles et des responsabilités (RACI, SOD pour PCI)

Définition de plan de tests de la conformité

Architecture de sécurité PCI DSS

Implement

Sensibilisation et retour d'expérience

Documentation des politiques et des procédures PCI DSS

Mise en œuvre des contrôles et mesures compensatoires

Operate

Gestion de la conformité PCI DSS via les services gérés

Externalisation stratégique et sécurisation du Cloud

Monitor

Evaluation des processus d'amélioration

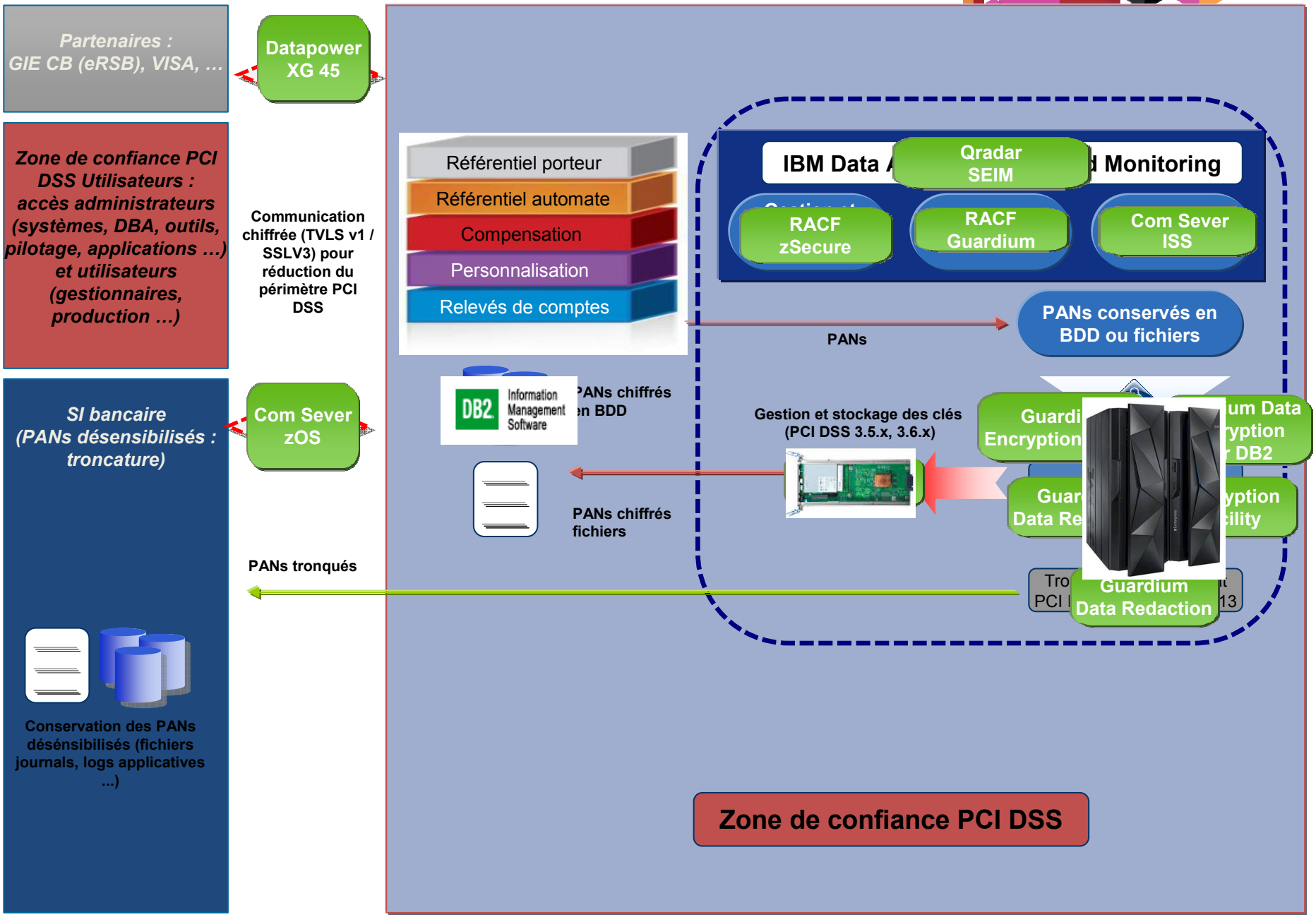
Performance des pratiques PCI DSS

Audit récurrents PCI DSS, PA-DSS

Un exemple d'architecture infrastructure : Protection des données cartes de crédit environnement bancaire

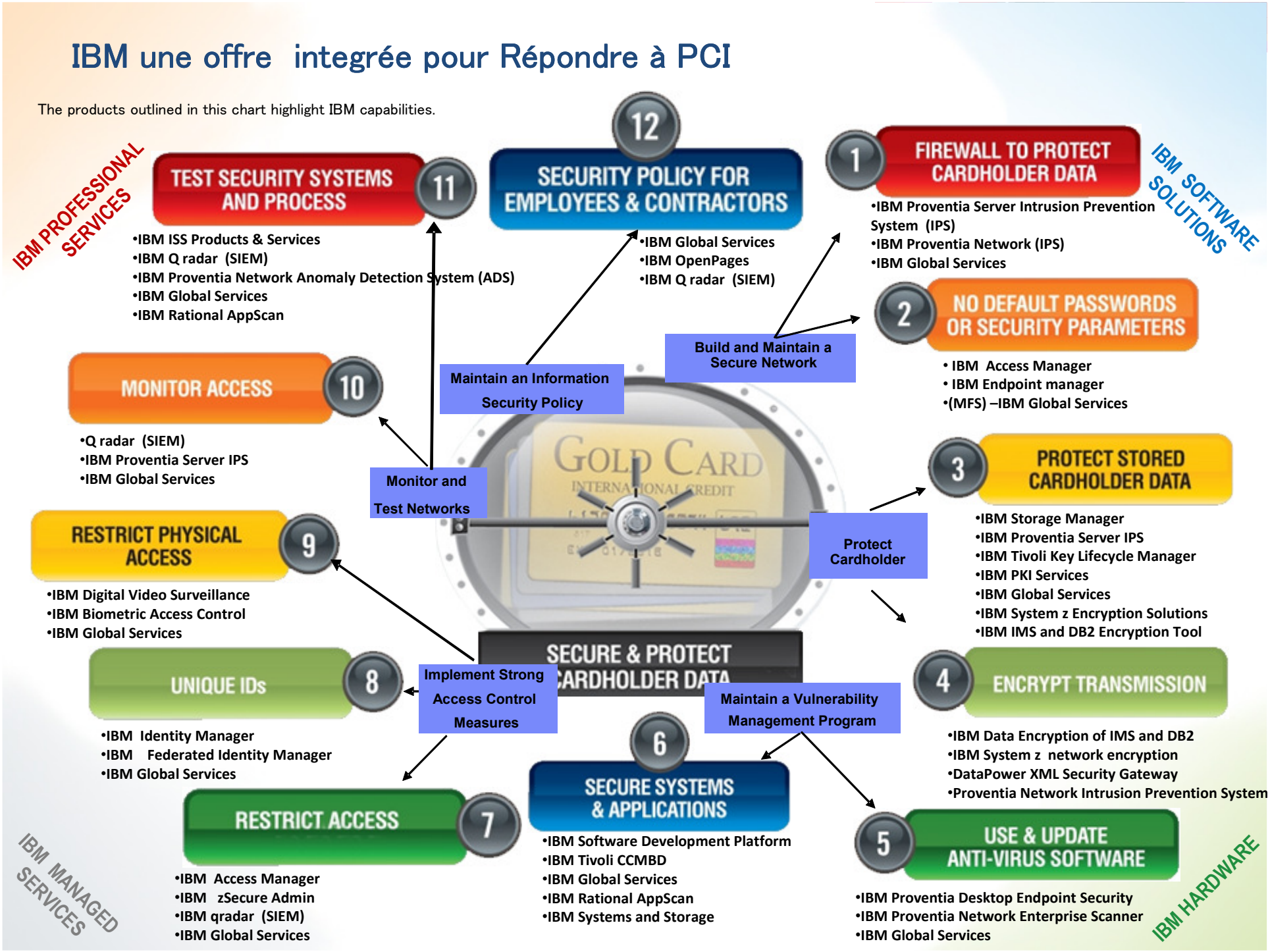
Question comment réaliser les conditions 3 et 4 en environnement bancaire mainframe ?

- Condition 3 : Protéger les données de titulaires de cartes stockées
- Condition 4 : Chiffrer la transmission des données des titulaires de cartes sur les réseaux publics ouverts


Partenaires :
GIE CB (eRSB), VISA, …
Datapower XG 45
Zone de confiance PCI DSS Utilisateurs : accès administrateurs (systèmes, DBA, outils, pilotage, applications …) et utilisateurs (gestionnaires, production …)
Communication chiffrée (TVLS v1 / SSLV3) pour réduction du périmètre PCI DSS
SI bancaire (PANs désensibilisés : troncature)
Com Sever zOS
Conservation des PANs désensibilisés (fichiers journals, logs applicatives ...)
Référentiel porteur
Référentiel automate
Compensation
Personnalisation
Relevés de comptes
IBM Data
Qradar SEIM
Monitoring
RACF zSecure
RACF Guardium
Com Sever ISS
PANs
PANs conservés en BDD ou fichiers
DB2 Information Management Software
PANs chiffrés en BDD
Gestion et stockage des clés (PCI DSS 3.5.x, 3.6.x)
PANs chiffrés fichiers
PANs tronqués
Guardium Data Redaction
Zone de confiance PCI DSS

IBM une offre integrée pour Répondre à PCI

The products outlined in this chart highlight IBM capabilities.




Questions ?!?