IBM

UNIVERSITÉ DU MAINFRAME

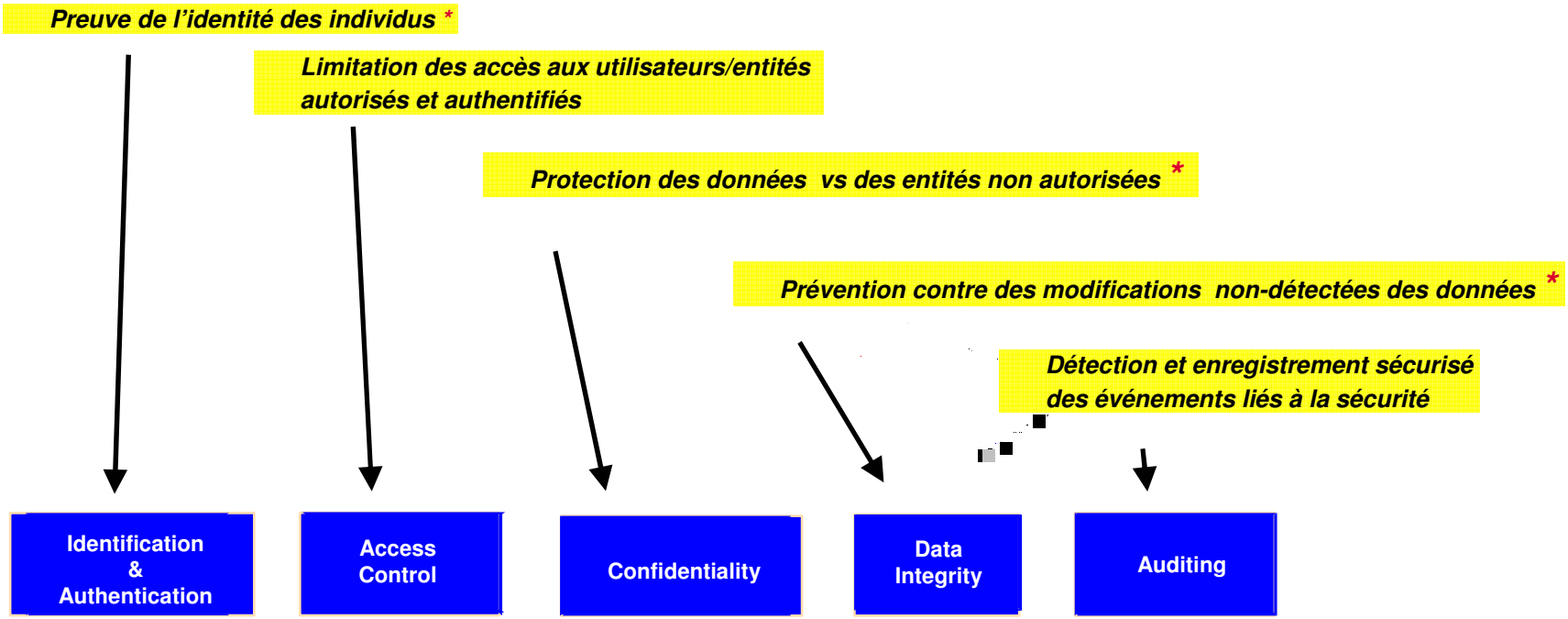
Sécurité et Chiffrement avec DB2 z/OS Version 8

Cécile BENHAMOU

Agenda

- **Nouveautés dans DB2 V8**
- **Support du Multi Level Security (MLS)**
- **Chiffrement DB2**
  - Fonctions construites DB2 V8
  - Encryption Tool

Une Définition de la Sécurité



Doit être implémenté comme une solution complète qui fournit

- **Un environnement informatique où l'on peut avoir confiance**
- **Intégrité de l'Information et des applications**
- **Conformité aux réglementations et limitation des risques**

L'endroit où vous mettez vos données à de l'importance….

Trust Authority

Data Vault

Sécurité dans toutes les couches du système
Sécurité des Transactions Online
Transmission internet sécurisée
Détection des intrusions préemptive
Collaboration avec les partenaires pour une sécurité dans l'entreprise étendue

Sécurité DB2: le besoin

- **Besoin d'être en conformité avec les réglementations**
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA); Health care
  - Gramm-Leach-Bliley Act of 1999 (GLBA); Financial services
    - . . .
  - Emergence des Storage Area Networks (SANs)
    - Besoin de stocker les données de façon sécurisée dans un environnement accessible de partout
- **Contrôle d'accès au niveau de la ligne nécessaire**
  - Web hosting
  - Confidentialité: des utilisateurs doivent pouvoir accéder seulement à un ensemble spécifique de lignes
    - Possibilité d'utiliser des vues
      - Difficile à gérer pour les UPDATE, INSERT, DELETE
      - Pas effectif pour les utilitaires

Sécurité DB2

- **Sécurité interne**
  - Utilisateurs authentifiés par RACF
  - Accès aux tables, Droit d'administration des Ressources DB2, Commandes DB2 gérées par ordres SQL

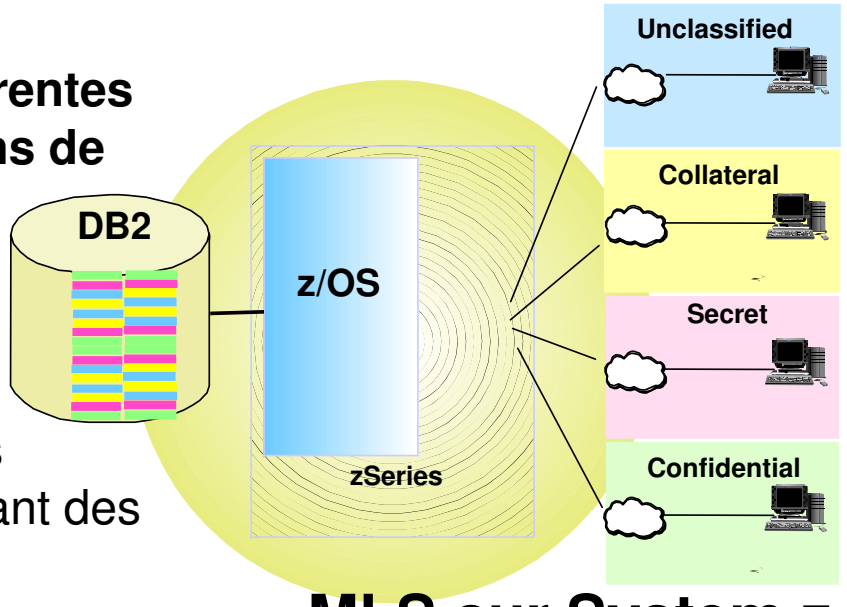
  - Sign-On sur console: utilisation du sign-on du user (au lieu de SYSOPR)
  - Commandes: GRANT à des Authids secondaires

- **Sécurité gérée par RACF**
  - Mise en oeuvre de l'exit DSNX@XAC
  - Utilisateurs authentifiés par RACF
  - Accès aux tables, Droit d'administration des Ressources DB2 via des Profiles RACF

  - Sign-On sur console: utilisation du sign-on du user (au lieu de SYSOPR)
  - Commandes DB2 gérées via des Profiles RACF

Multi Level Security (MLS)

BESOIN: Partager des données entre différentes personnes/organisations avec des "besoins de savoir" différents



MLS sur System z

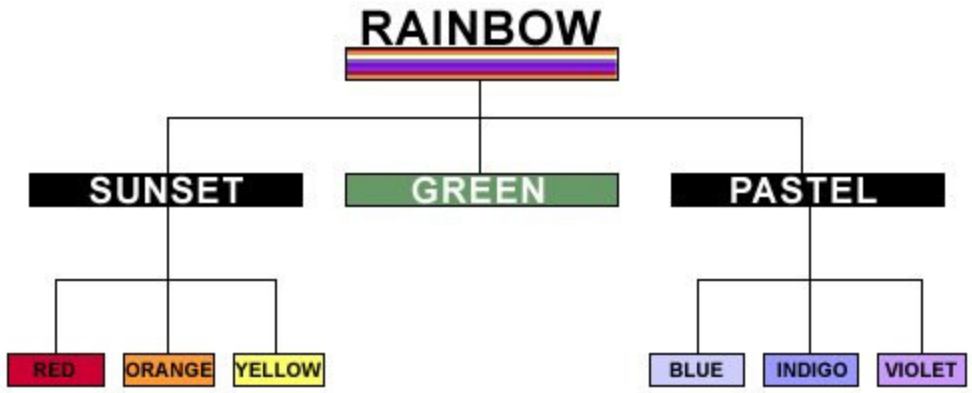
MLS

- Un repository UNIQUE contient des attributs différents accessibles par des utilisateurs ayant des autorisations de niveaux différents.
- Empêche la déclassification (Write-Down) des données sauf si autorisation explicite
- Elimine le besoin d'infrastructures isolées ou dupliquées pour garantir la sécurité

Une image des données UNIQUE
partageable par plusieurs départements de l'entreprise avec différents niveaux d'autorisation.

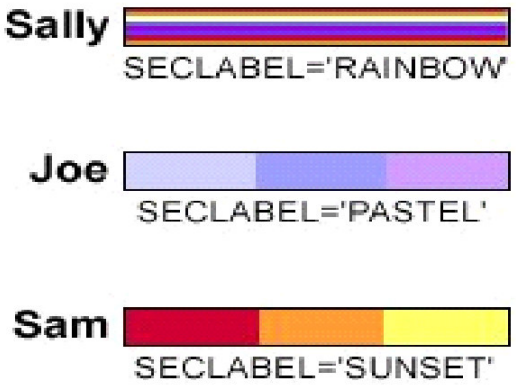
Multi Level Security (MLS)

- **Mise en oeuvre dans RACF**
  - Mise en oeuvre d'une sécurité hiérarchique (SECLEVEL) et de catégories (CATEGORY)
  - La classe SECLABEL doit être active
  - Assignation de label de sécurité aux utilisateurs
- **Comparaisons SECLABEL**
  - Dominance
  - Reverse dominance
  - Equivalence
  - Null
- **Write down**



DB2 V8 et Sécurité Multi-Niveaux (MLS)

►Colonne dans la table définie AS SECURITY LABEL
- chaque ligne a un label de sécurité spécifique
- le label de sécurité est obtenu de RACF



DB2_ SECURITY_ LABEL_EXT	COL1	COL2	COL2
RAINBOW	56	7	76
RAINBOW	24	56	65
RAINBOW	42	6	45
BLUE	3	456	7
INDIGO	113	456	56
VIOLET	3	456	4
BLUE	4	4556	7
RED	4	76	567
ORANGE	33	7	567
RED	5455	76	567
YELLOW	999	65	45

Un utilisateur avec une autorisation RAINBOW aura le droit d'accéder à toutes les lignes
Un utilisateur avec une autorisation PASTEL aura le droit d'accéder aux lignes PASTEL, BLUE, INDIGO, VIOLET

DB2 V8 et Sécurité Multi-Niveaux (MLS): mise à jour d'une table

- Privilège "Write-Down"
  - Défini dans RACF
  - Permet de déclassifier une information (changer son label de sécurité)

- INSERT
  - ligne insérée avec label de sécurité de l'utilisateur par défaut
  - si privilège "Write-Down", l'utilisateur peut mettre n'importe quel label de sécurité

- UPDATE
  - ligne mise à jour si label de sécurité de l'utilisateur équivalent à celui de la ligne
  - si privilège "Write-Down", l'utilisateur peut mettre n'importe quel label de sécurité

- DELETE
  - ligne supprimée si label de sécurité de l'utilisateur équivalent à celui de la ligne
  - si privilège "Write-Down", l'utilisateur peut supprimer les lignes avec un label de sécurité inférieur

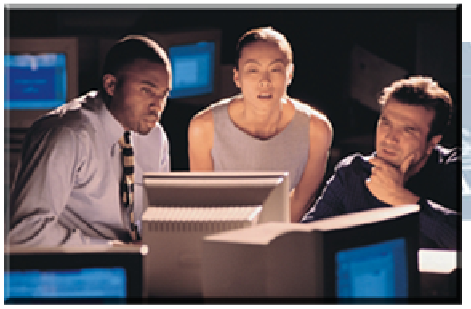
DB2 V8 et Sécurité Multi-Niveaux (MLS): utilitaires

- LOAD RESUME
  - ligne insérée si label de sécurité de l'utilisateur équivalent à celui de la ligne
  - si privilège "Write-Down", l'utilisateur peut mettre n'importe quel label de sécurité
- LOAD REPLACE
  - Privilège "Write-Down" nécessaire
- UNLOAD ou REORG UNLOAD EXTERNAL
  - ligne déchargée si label de sécurité < ou = au label de sécurité de l'utilisateur
- REORG DISCARD
  - ligne supprimée si
    - les labels de sécurité de la ligne et de l'utilisateur sont équivalents
    - si l'utilisateur a un privilège "Write-Down" et que la ligne à un label de sécurité inférieur ou égal

DB2 V8 et Sécurité Multi-Niveaux (MLS)

- **Prérequis**
  - z/OS 1.5 et Security Server (RACF) V1R5
- **Restrictions**
  - Sécurité niveau ligne non prise en compte (enforced) quand DB2 vérifie les contraintes référentielles
  - Contraintes référentielles, FIELDPROC, EDITPROC, check constraints, ne peuvent pas être définies sur une colonne SECLABEL
  - Les requêtes sur une table définie avec un label de sécurité ne peuvent pas utiliser le parallélisme.

Le Pouvoir de l'encryption du Mainframe



Aider à protéger vos données à travers Internet

Objectifs clients:

- **Seules les personnes autorisées peuvent décrypter**
- **Disponibilité des clés et services de décryptage quand on en a besoin**

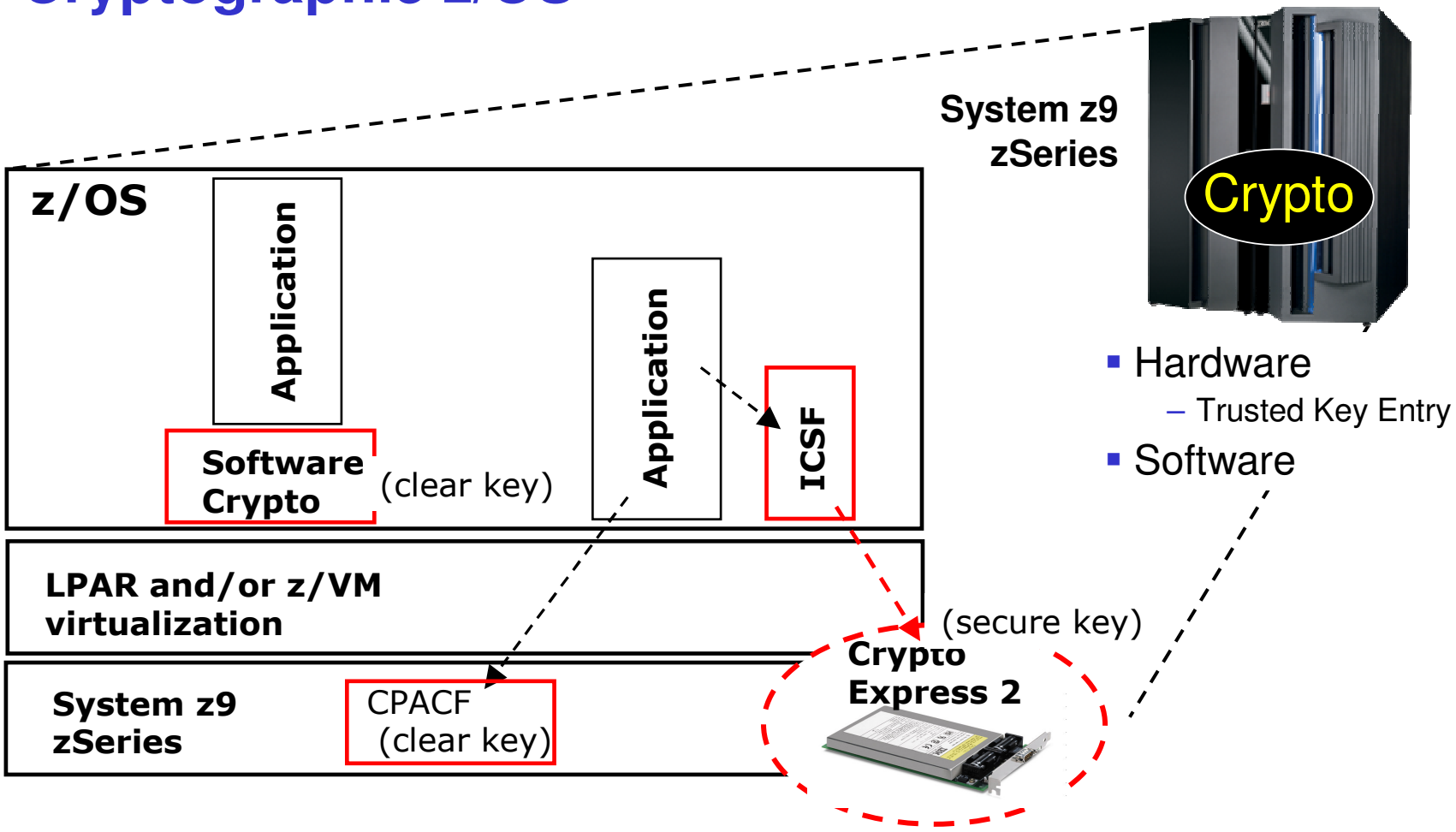
Gestion des clés centralisée

Aider à protéger vos données quittant votre entreprise

Aider à protéger vos données archivées

- IBM Encryption Facility for z/OS announce dates:
  - Encryption Services – 28 Oct, 2005
  - DFSMSdss Encryption - 2 Dec, 2005

Cryptographie z/OS



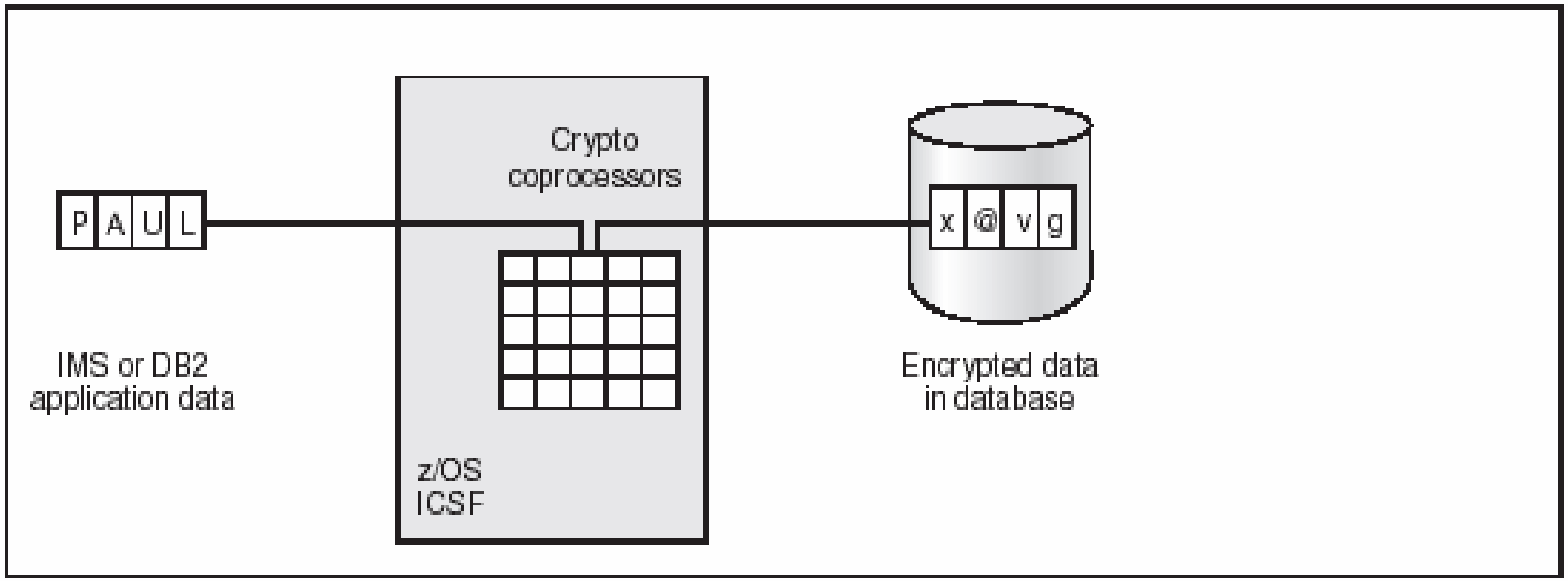
Crypto accessible via multiple language paths; from assembler for clear key crypto to CCA, OCSF, and Java interfaces to secure key HW assisted crypto.

DB2 et le chiffrement (encryption)

- **2 possibilités**
  - DB2 V8: Fonctions construites
  - IBM Data Encryption Tool for DB2 and IMS Databases

- **Méthodes très différentes**
  - Niveau de chiffrement:
    - Colonne avec DB2 V8
    - Ligne avec Encryption Tool
  - Qu'est ce qui est chiffré?
    - Données et Index avec DB2 V8
    - Données uniquement avec Encryption Tool
  - Modifications des Applications
    - Importantes avec DB2 V8 (Utilisation des fonctions construites dans les ordres SQL)
    - Aucune avec l'Encryption Tool (utilisation EDITPROC)

Chiffrement des données



Pendant le chiffrement, les données des applications IMS ou DB2 (″paul″) sont converties en des données incompréhensibles (″x@vg″) à part à la personne qui a la clé de chiffrement (encryption key label) et peut donc déchiffrer les données. La clé de chiffrement est attribuée par l'administrateur de sécurité.
Le déchiffrage est le processus inverse, prenant les données de la base (“x@vg”) et les convertissant dans leur forme initiale (“paul”).

Chiffrement DB2 V8: fonctions construites

- Chiffrement des Données et des Index

- Chiffrement au niveau de la colonne

- Colonnes définies en VARCHAR FOR BIT DATA avec la longueur nécessaire pour stocker la clé (et doit être un multiple de 8)
- Par exemple: pour une colonne définie en VARCHAR(6):
  - Maximum length of non-encrypted data 6 bytes
  - Number of bytes to the next multiple of 8 2 bytes
  - 24 bytes for encryption key 24 bytes
  - Total Encrypted data column length 32 bytes

- CREATE TABLE EMP (EMPNO VARCHAR(32) FOR BIT DATA)

Chiffrement DB2 V8: fonctions construites

- Mot de passe pour le Chiffrement
  - ►SET ENCRYPTION PASSWORD = :hv_pass

- Utilisation du mot clé ENCRYPT pour insérer des données chiffrées:
  - INSERT INTO EMP (EMPNO) VALUES(ENCRYPT('47138'))

- Afficher une colonne avec les données déchiffrées:
  - SELECT DECRYPT_CHAR(EMPNO,:hv_pass) FROM EMP
    - Si mot de passe correct, DB2 retourne le numéro d'employé déchiffré
    - Remarque: On peut utiliser le registre spécial SET ENCRYPTION PASSWORD pour fournir le mot de passe

- GETHINT: fournit un indice permettant de se rappeler le mot de passe

Chiffrement DB2 V8 : remarques et restrictions

- Données CHAR et VARCHAR directement supportées. Données Numériques et Timestamp supportées indirectement via le casting.

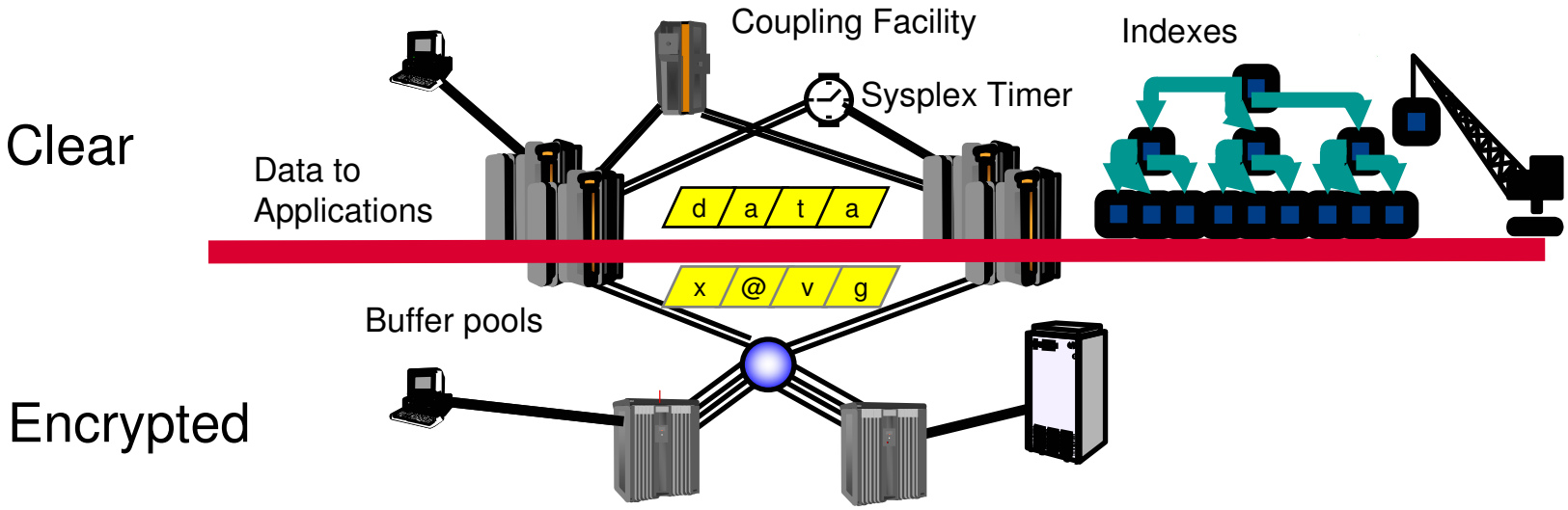
- LOAD et UNLOAD: ne supportent pas le chiffrement DB2
- Programmes SQL (comme DSNTIAUL): supporte le chiffrement DB2

- Performances:
  - Si un prédicat demande du déchiffrement, il est de ‘stage 2’
  - La vérification de plage sur des données chiffrées nécessite un tablespace scan. En effet, ce sont des données binaires qui nécessitent toutes les valeurs d’une ligne pour déchiffrer la colonne.

.

Outil “IBM Data Encryption for IMS and DB2 Databases”

- Chiffrement des données sur disque (données au repos)
  - Données sur les canaux chiffrées (protection contre les attaques sur les canaux/réseaux)
  - Données dans les buffers non chiffrées
- Contrôles d'autorisation existants sur les accès à ces données ne sont pas affectés



- **Exploite les dispositifs matériel Crypto des System z**

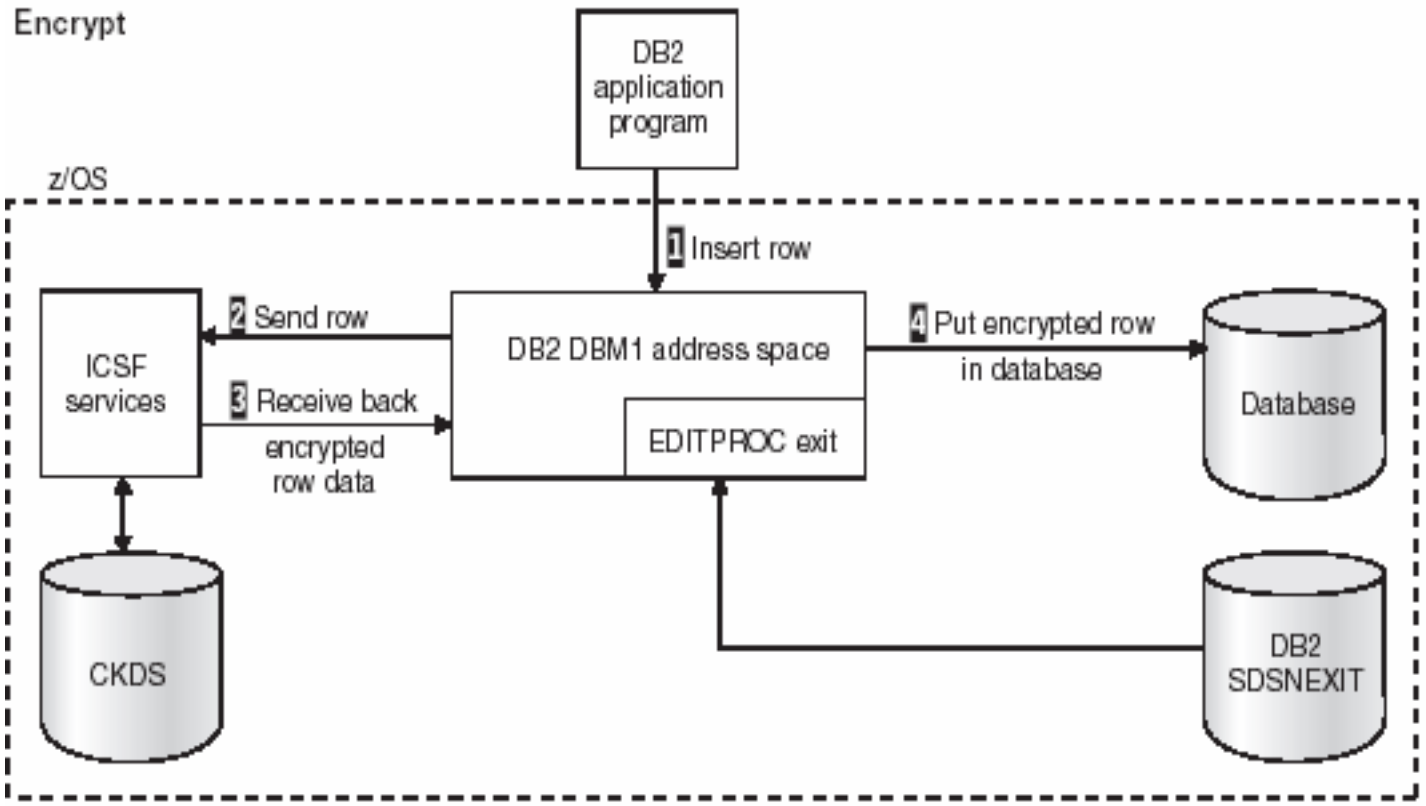
Outil “IBM Data Encryption for IMS and DB2 Databases”

- Utilise l’algorithme “ANSI Data Encryption Algorithm” (DEA), aussi connu sous le nom de “U.S. National Institute of Science and Technology (NIST) Data Encryption Standard (DES)”
- Le DES simple ou triple (qui donne un niveau de protection plus élevé) peut être utilisé.

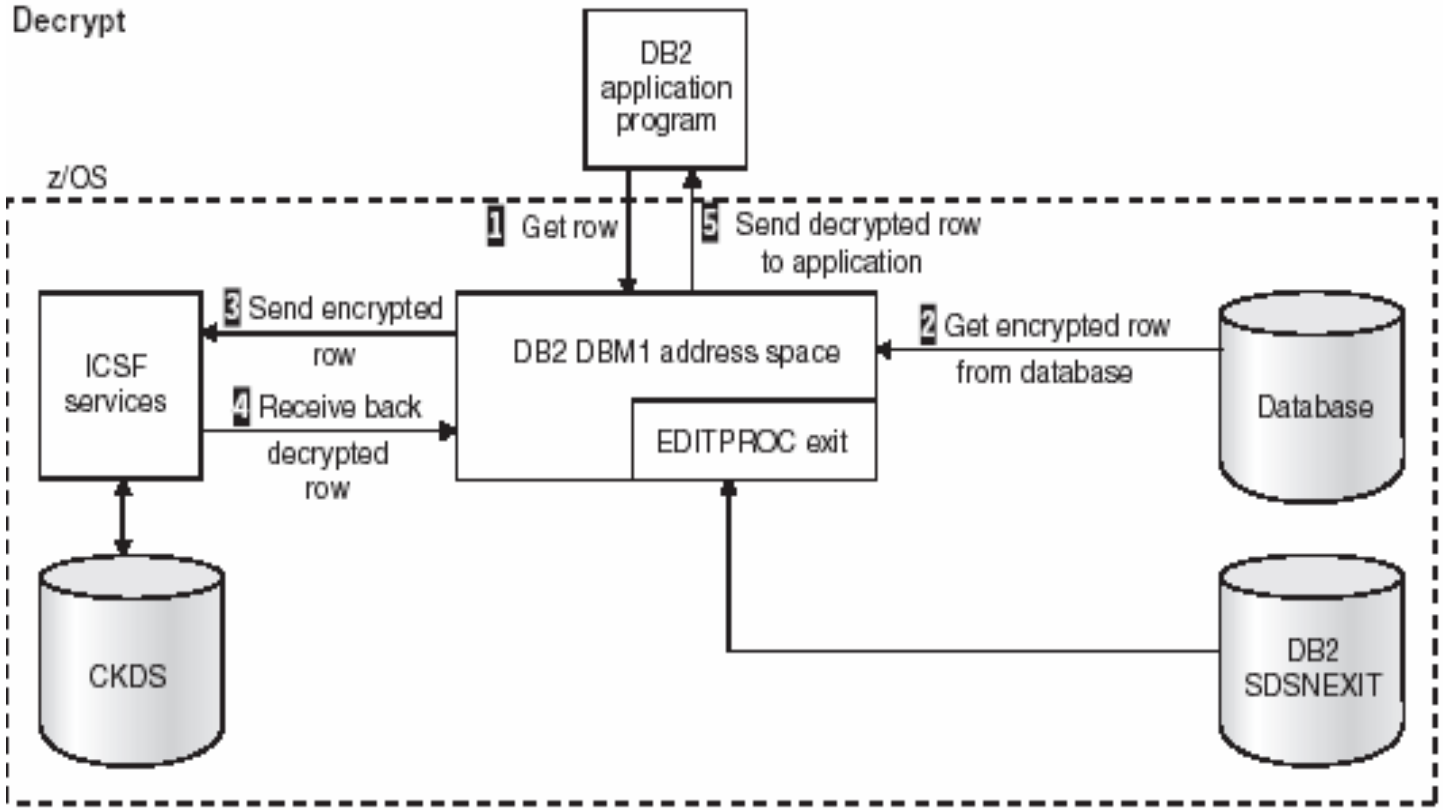
- Exploite les ‘features’ cryptographiques des system z pour éviter l’overhead du chiffrement/déchiffrement

- Utilise une EDITPROC. Celle-ci chiffre les données à l’insertion (et lors de mise à jour) et les déchiffre au moment de la sélection.

IBM Data Encryption Tool for DB2 and IMS Databases - Chiffrement



IBM Data Encryption Tool for DB2 and IMS Databases - Déchiffrement



IBM Data Encryption Tool for DB2 and IMS Databases: mise en oeuvre

- **Mise en oeuvre de Integrated Cryptographic Service Facility (ICSF).**
  - Configuration hardware configuration
  - Mise en oeuvre de la clé système maitre
- **Génération et stockage de la clé DES**

- **Construction de l'exit: elle doit spécifier le label clé de chiffrement généré.**
- **Sauvegarder les données**
- **Décharger les données**
- **Recréer la table avec l'exit.**
- **Recharger les données (elles vont être chiffrées)**
- **Valider une sélection de données**

IBM Data Encryption Tool for DB2 and IMS Databases

- **Prérequis**
  - OS/390 or z/OS Integrated Cryptographic Service Facility (ICSF)
  - DB2 for OS/390 Version 6 ou plus, et/ou IMS Version 6 ou plus
- **Considérations**
  - Possibilité de définir autant de clés de chiffrement que l'on veut (elles sont définies par l'administrateur de sécurité). Une exit doit être construite pour chaque clé de chiffrement définie
  - On peut chiffrer et compresser les données en utilisant la compression hardware. Toutefois, la compression a lieu après le chiffrement, ce qui a pour effet de diminuer son efficacité.
- **Restrictions liées à l'EDITPROC:**
  - Pas de modifications sur la structure de table (ajout de colonne, …)
  - Pas de colonne LOB, ROWID ou Identity.

Chiffrement: DB2 V8 ou Data Encryption Tool ?

- Comparaisons

Chiffrement DB2	IBM Data Encryption Tool for DB2 and IMS Databases
Niveau Colonne	Niveau Ligne
Type de colonne doit être modifié VARCHAR FOR BIT DATA	Utilisation EDITPROC
Données et Index	Données uniquement
LOAD et UNLOAD ne supporte pas le chiffrement	LOAD et UNLOAD supporte le chiffrement

Chiffrement: Documentation

- IBM Data Encryption Tool for IMS and DB2 Databases User Guide - SC18-7336-02
- IBM Encryption Tool for DB2 and IMS White Paper – Jeff Berger and Jeff Novak SVL
- Activating S/390 and zSeries Cryptographic Services for the IBM Data Encryption for IMS and DB2 Databases – Pete Sexton SVL
  - available at www.software.ibm.com/data/db2imstools
- The ICSF System Programmer's Guide and the other ICSF books can be found online at one of the following locations. Search on books with titles containing 'ICSF'
  - http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/zos/zbop3_srch.html#titles
  - For z/OS:S/390 Crypto PCI Implementation Guide, SG24-5942-00
- Exploiting S/390 Hardware Cryptography with Trusted Key Entry, SG24-5455-00
- DB2 UDB for z/OS V8 Performance Topics – SG24-6465-00