Optimisation de l'espace mémoire du DMP par compression des transactions médicales

par

Rachid Osmar ZAÏANE

et

André GAMACHE

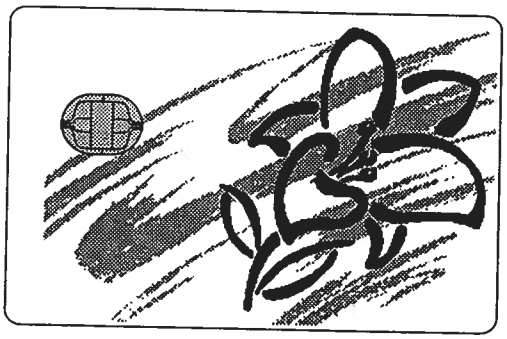
Université Laval - Québec

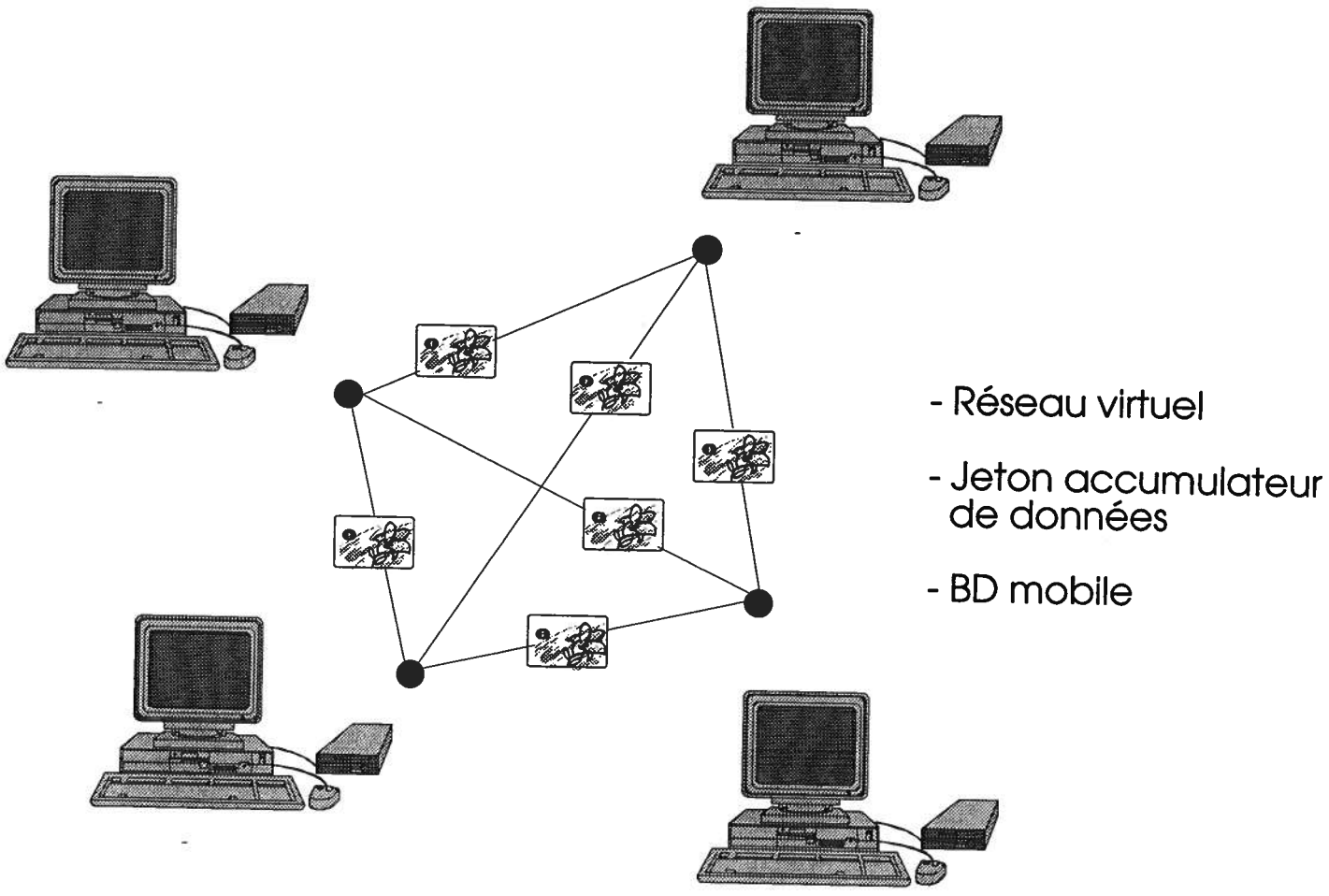
ACFAS 1993 - Rimouski Québec

- Dossier Médical Portable

Carte à microprocesseur

Mémoire EEPROM **8 KOctets**



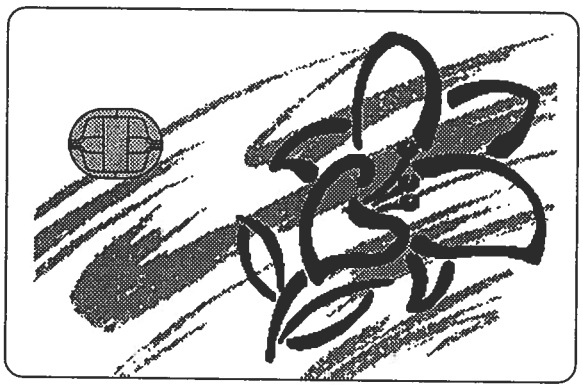


- Réseau virtuel
- Jeton accumulateur de données
- BD mobile

DMP structuré par tables

R1

R2



R3

R4

Transactions médicales caractérisées par des enregistrements de petite taille

R2

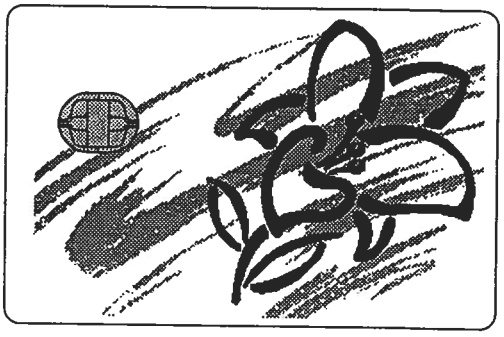
C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{23}

R1

C_{11}	C_{12}	C_{13}
C_{11}	C_{12}	C_{13}
C_{11}	C_{12}	C_{13}

R3

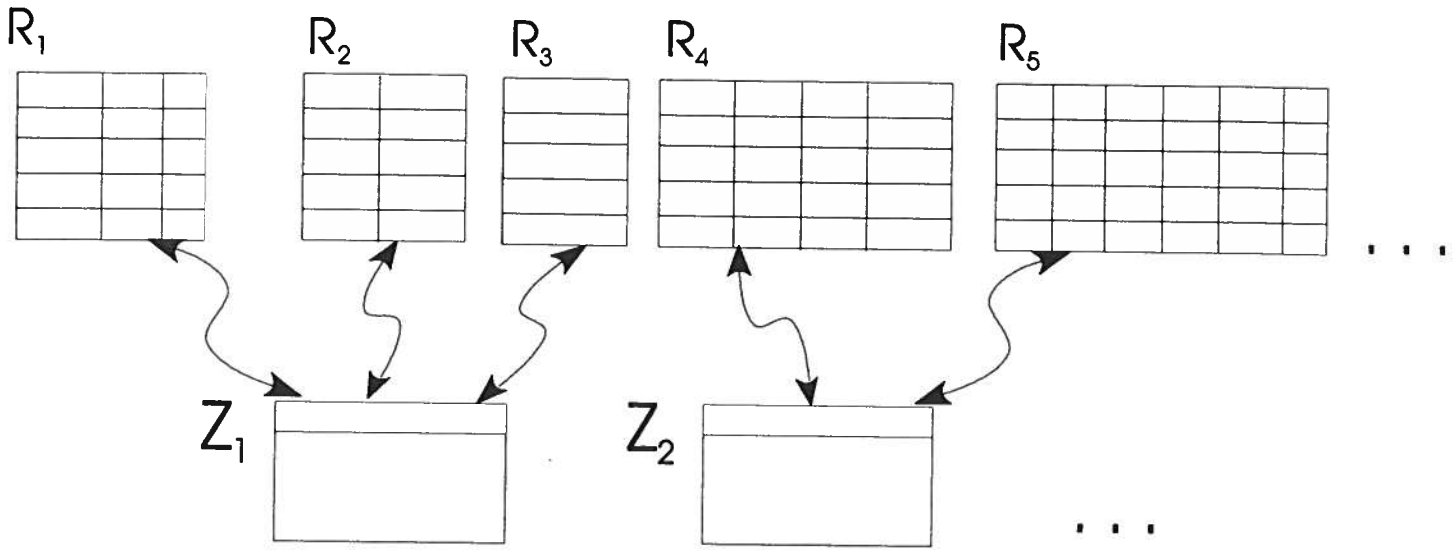
C_{31}



R4

C_{41}	C_{42}
C_{41}	C_{42}

Association des tables par blocs



$\mathcal{R}$ = { R_1, R_2, . . . } ensemble des relations
(tables)
(zones logiques)

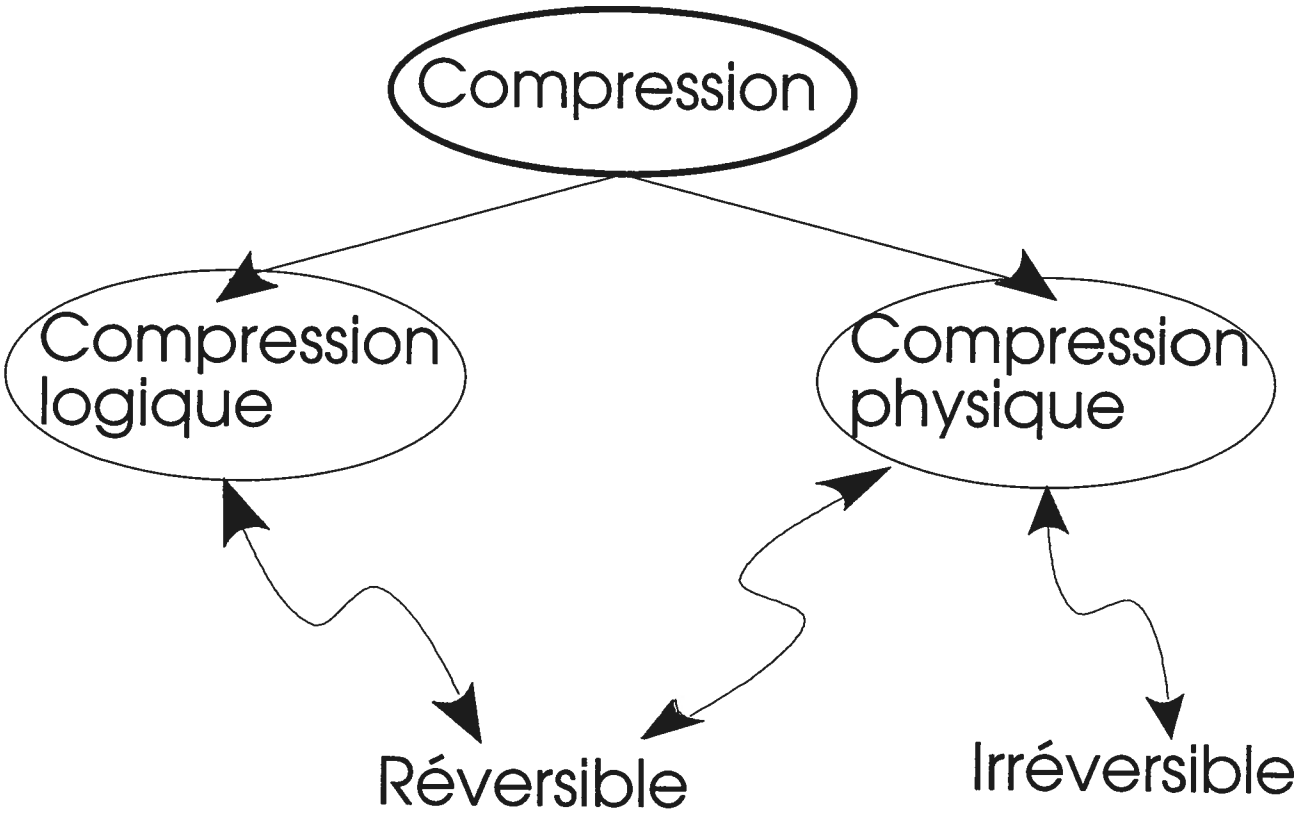
$\mathcal{Z}$ = { Z_1, Z_2, . . .} ensemble de blocs mémoire
(zones physiques)

Cardinal de $\mathcal{R}$ > Cardinal de $\mathcal{Z}$

$\mathcal{P}(Z_i)$ = Protection octroyée à une zone physique

$\mathcal{P}(Z_i) \# \mathcal{P}(Z_j)$ si i # j

Familles d'algorithmes



Compression Logique: liens logiques entre les données

☞ **Liée au contexte**

Compression Physique: calcul des fréquences d'apparition

☞ **Pour de gros "corpus"**

☞ ex: Huffman, LZW, LZHUF ...

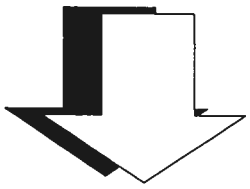
Le contexte

DMP = { R_1, R_2, R_3, ... , R_n}

où R_i est une relation (ou zone logique)

$\forall$ i R = {C_1,C_2, C_3, ... C_m}

où C_i est un champ de type **T** définit dans un domaine **D**



Dictionnaire de définition du DMP

Dictionnaire de contexte

Il contient la structure du DMP
- association Champs-Types
- regroupement des relations par zones

Types et Domaines

Types génériques	Types spécifiques
Booléen	1 à 31 bits
Entier	1, 7, 15, 31, 63, 127, 255, 511, 1023 2047, 4045, 8191, 16383, 32767, 65535, 131071, 621441, 1242883, 2485767
Réel	9.9, 9.99, 9.999, 99.9, 99.99, 99.999, 999.9, 999.99, 999.999, (9).(9)
Chaîne de caractères	fixe ou taille variable BCD, ISO5, ISO6, ASCII7, ASCII
Date	siècle + année + mois + jour année + mois + jour mois + jour déplacement dans une période
Liste simple	
Structure	
Liste structurée	

Transaction médicale

@champ$_1$@champ$_2$@champ$_3$@...@champ$_n$

|sous_champ$_1$|sous_champ$_2$|...

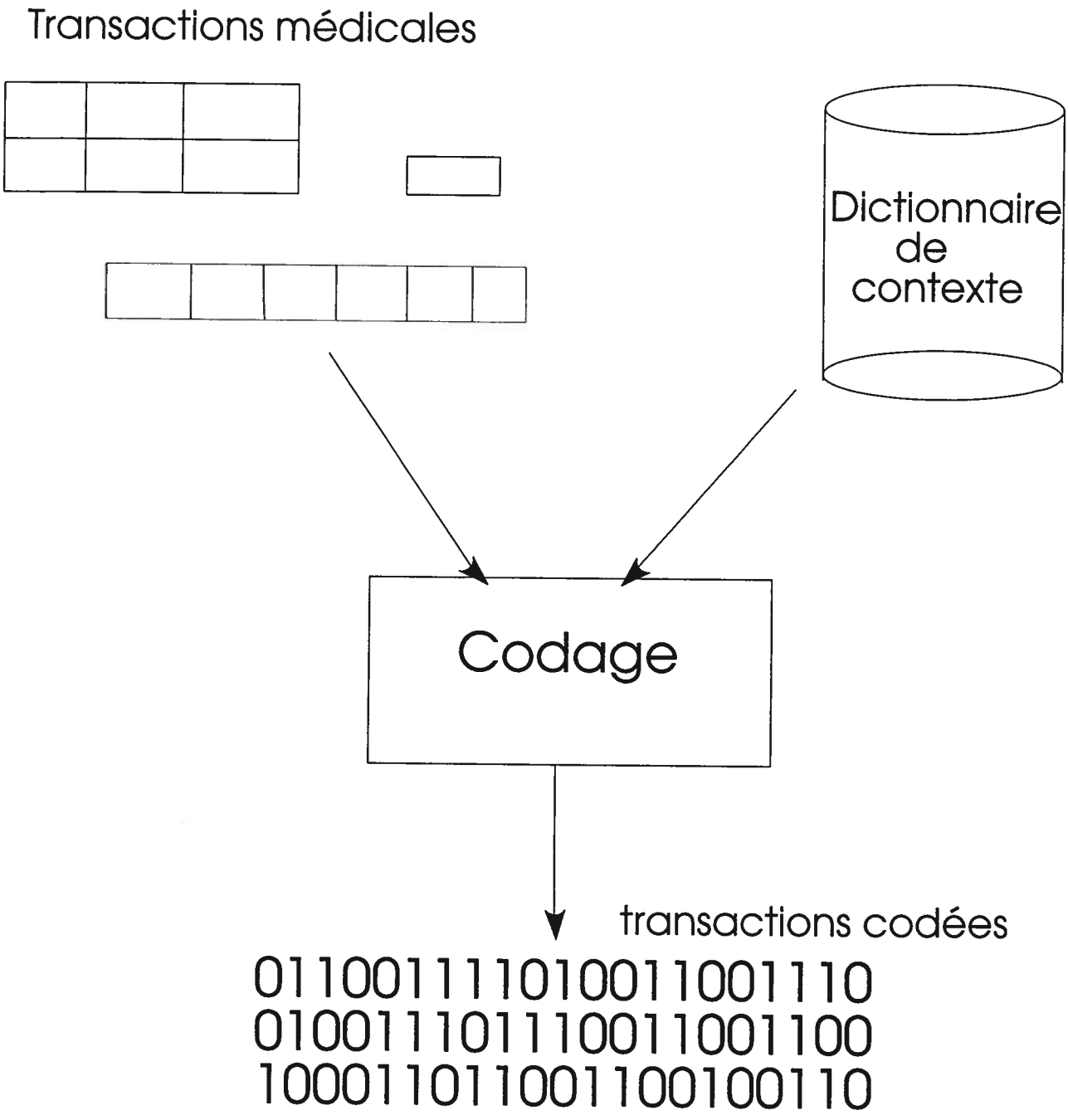
~infra_champ$_1$~infra_champ$_2$~...

@1@T9150.@56@930520@00912345

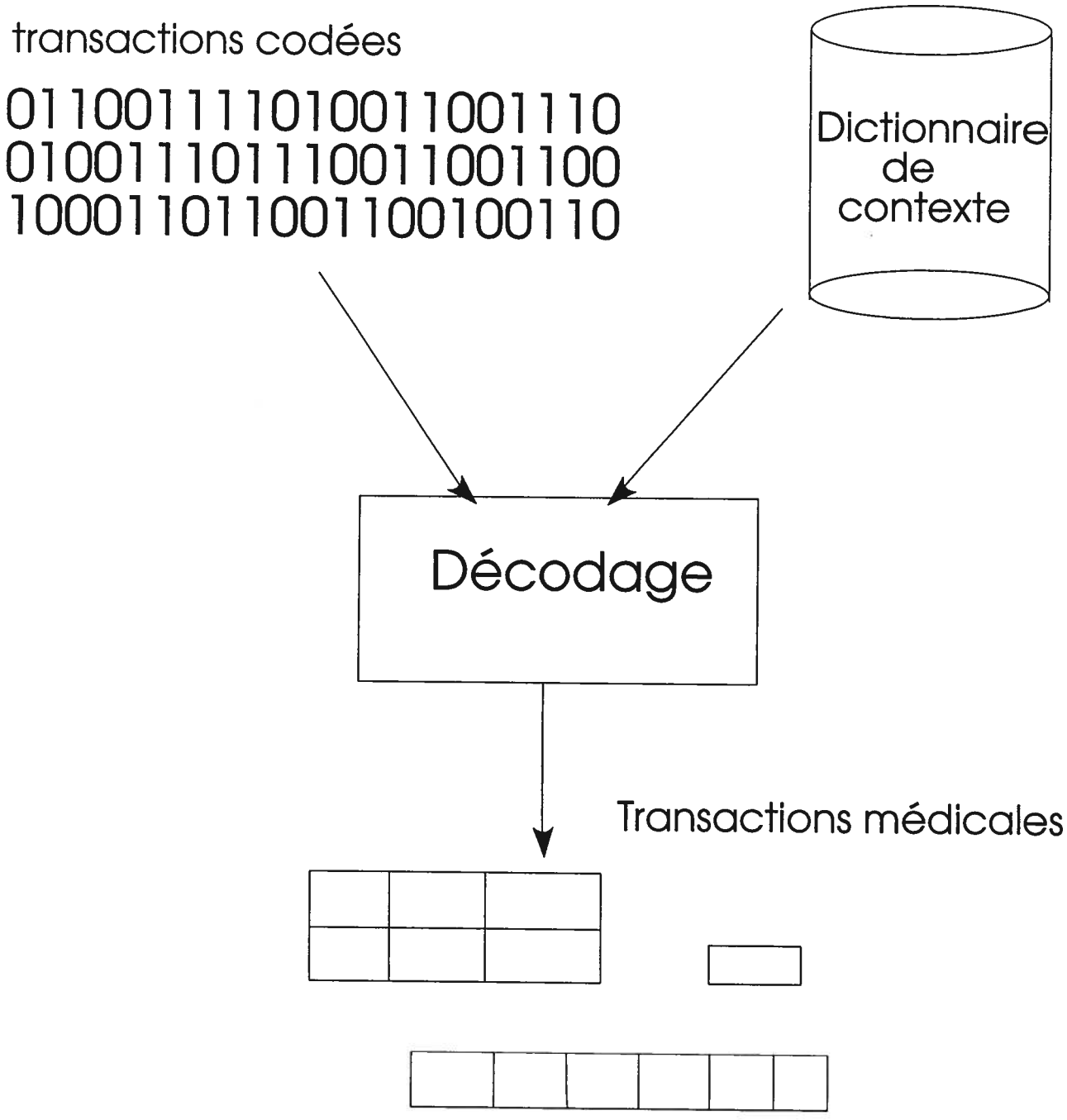
@|0|1|3|0|1|2@|6|5@|0|1|0|0|0|1|1|1|0|1@
|6|6@930520@00912345

@1@A7832.@@|~J~10|~J~10|~E~7@|19|5|2|1@
|47|53|12|1|24@930520@00912345

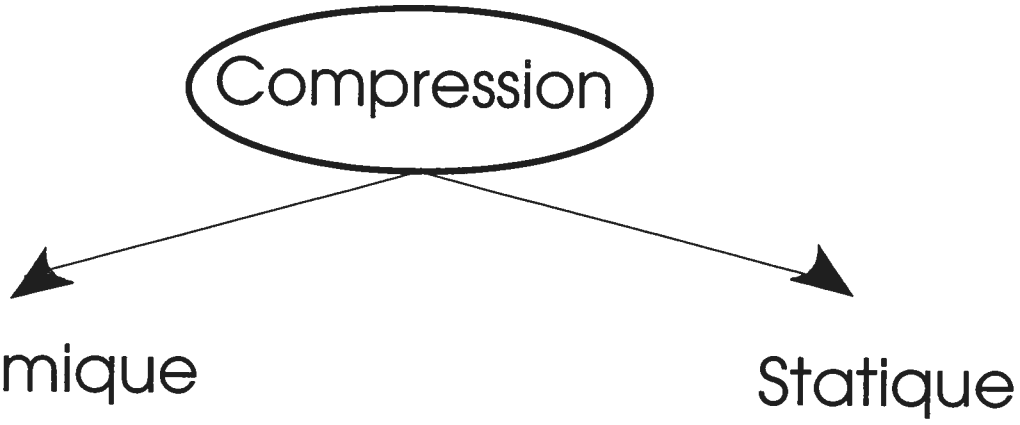
Compression



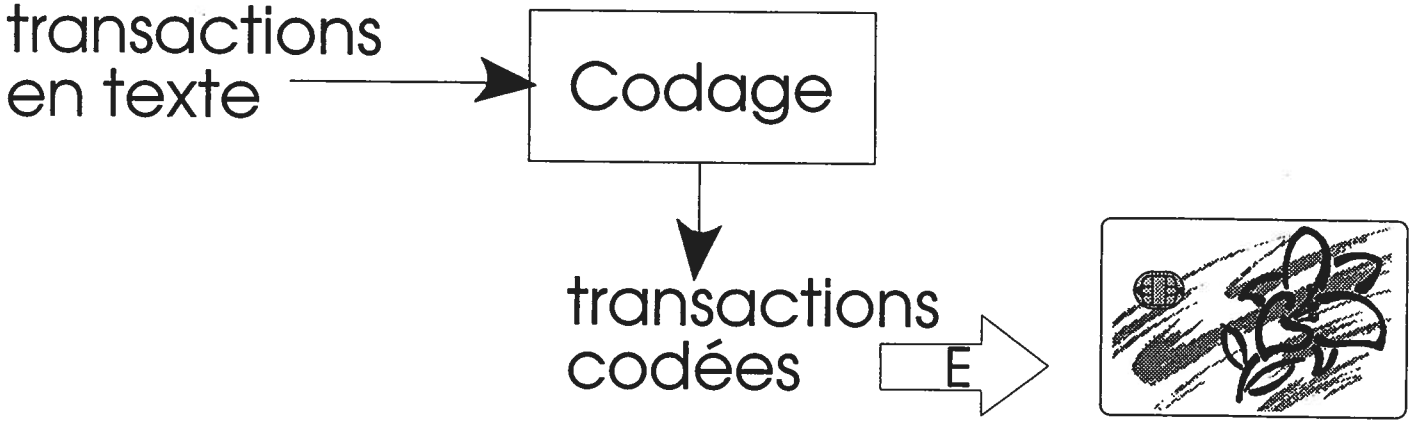
Décompression



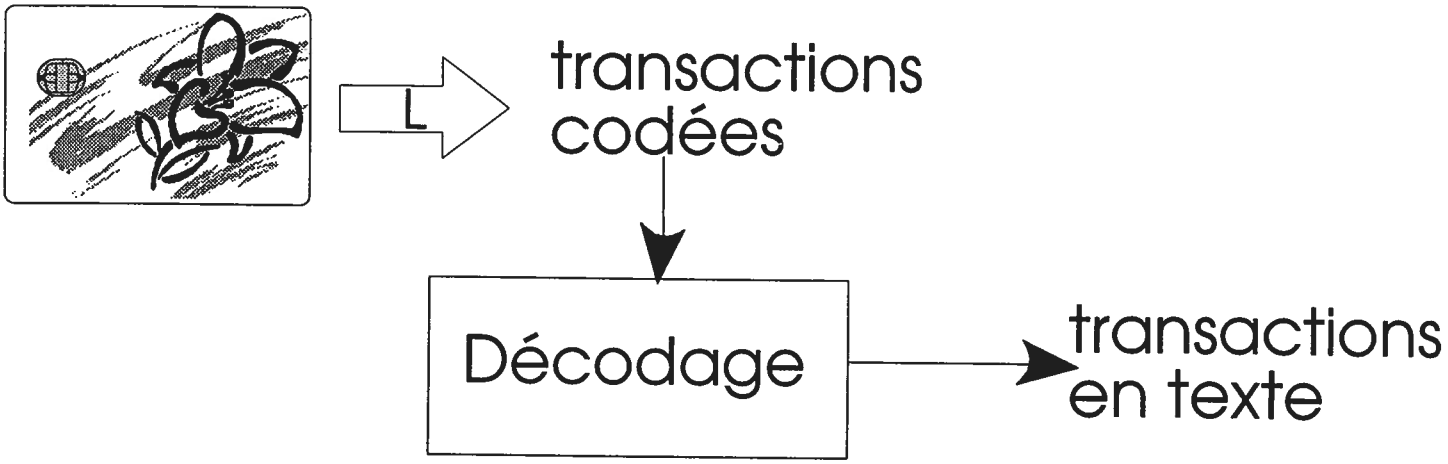
Compression et décompression à la volée



Ecriture:



Lecture:



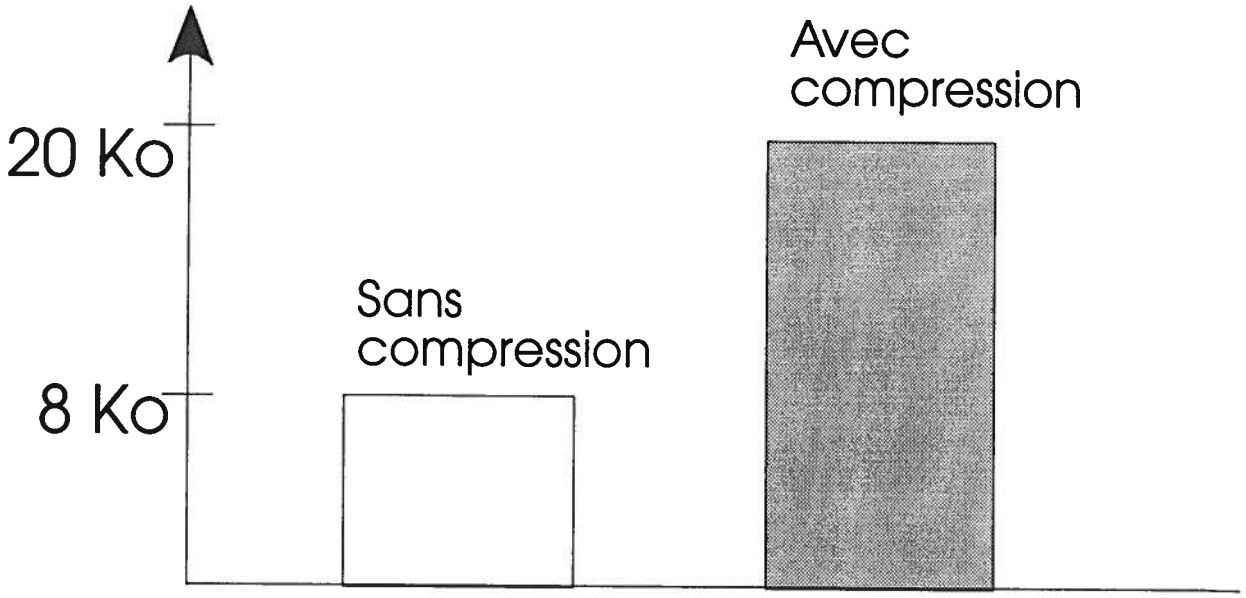
Avantages

- Diminution de la taille des données
- Augmentation de la capacité de la carte
- Diminution du temps de transfert des données
- Chiffrement des données sur la carte

Inconvénients

- Implantation plus complexe à gérer
- Données plus sensibles

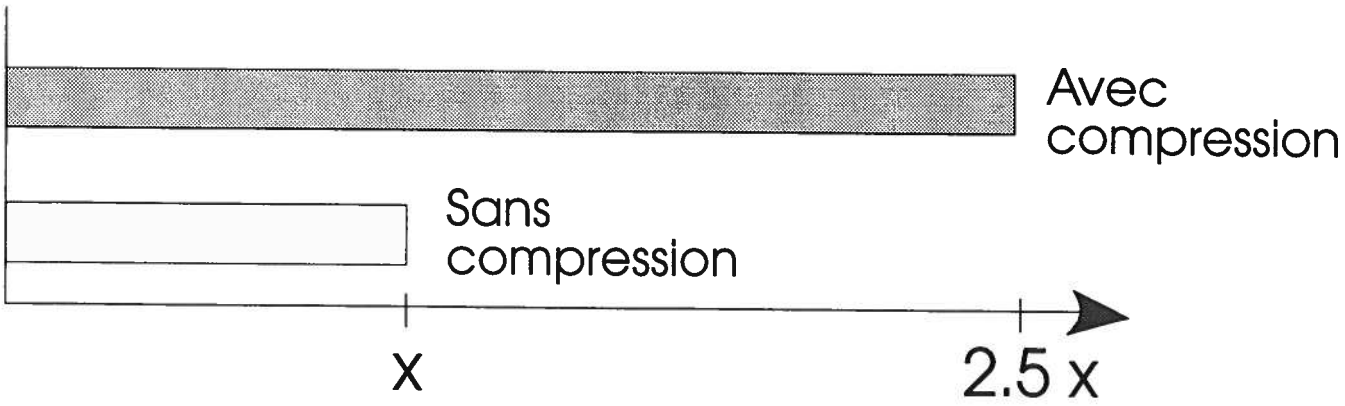
Résultats



Capacité moyenne de la carte

Gain minimum d'espace = 34.33 %

Gain maximum d'espace = 94.85 %

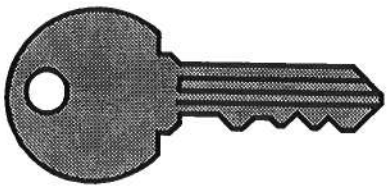


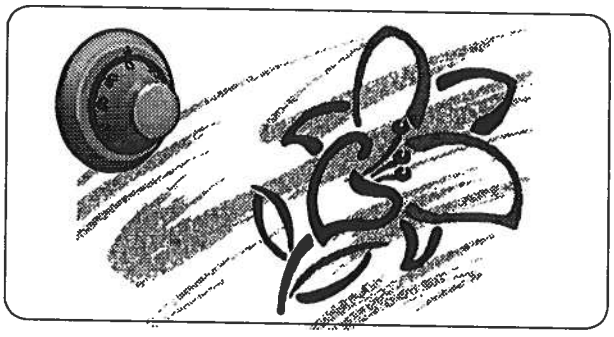
Durée du cycle de vie de la carte

La sécurisation des échanges avec la Carte Santé et le projet de Rimouski

Rachid Zaïane et André Gamache

Département d'informatique
Faculté des Sciences et de Génie
Université Laval
e-mail: gamache@vm1.ulaval.ca





Acfas 1993

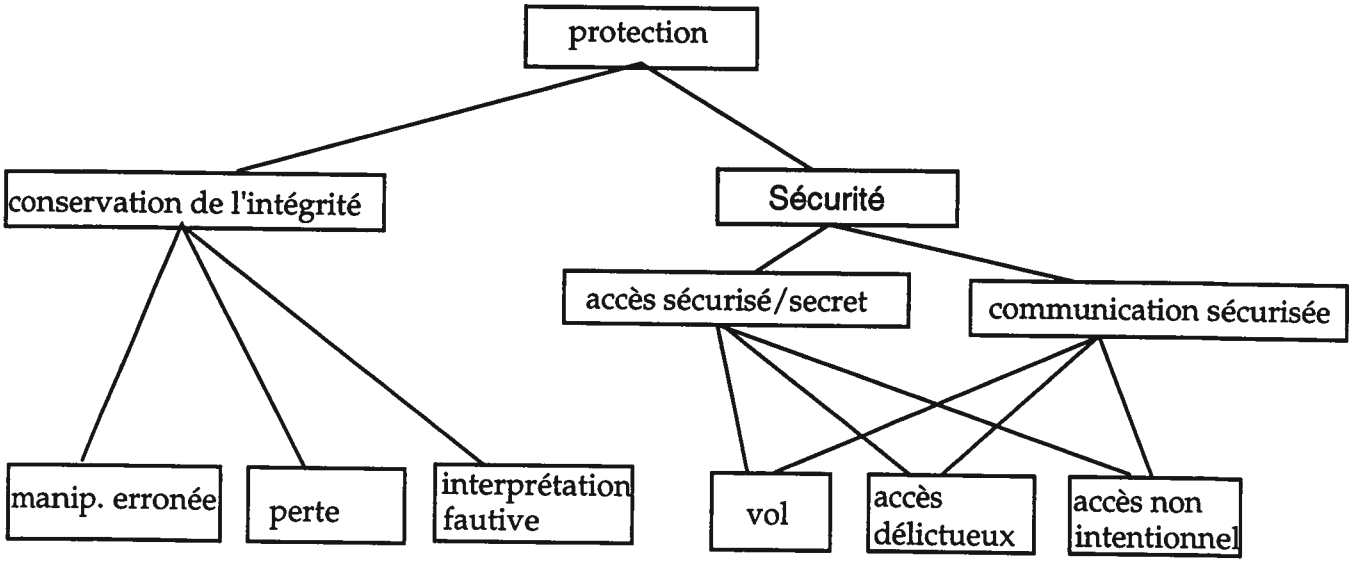
Colloque du 20 mai 1993

Protection des données: implications et effets

deux facettes :

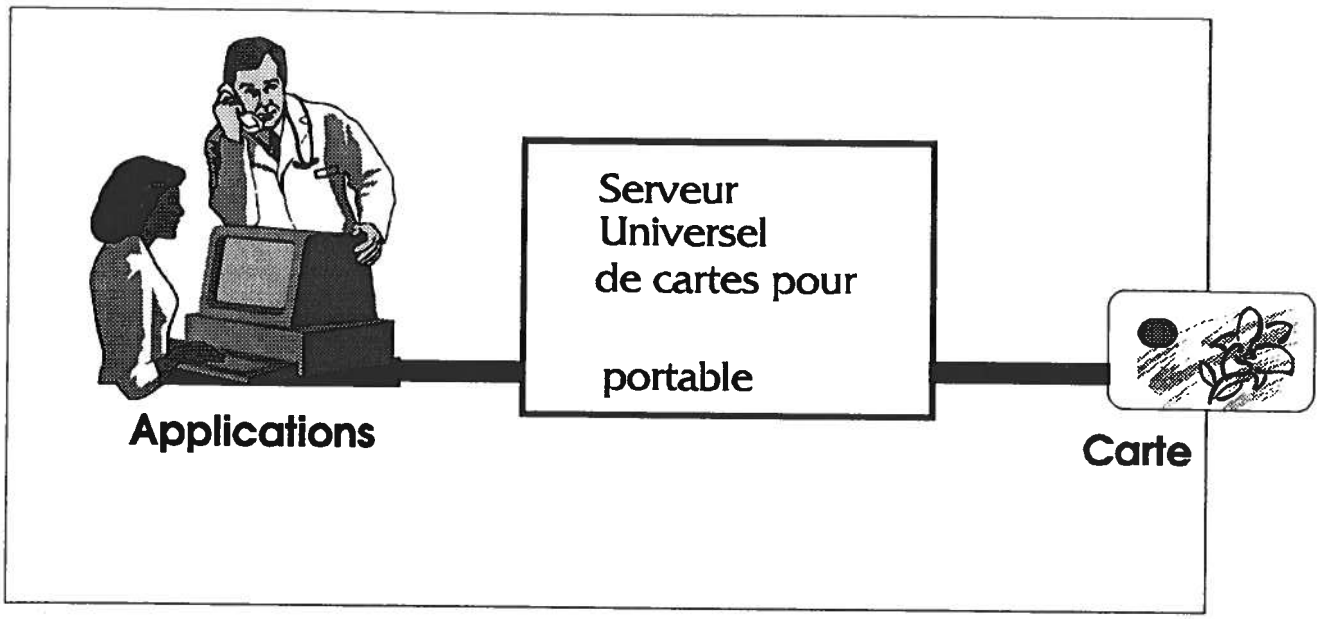
sécurité : accès autorisés seulement

intégrité: données valides et complètes



GriesserC. G. et al. Data protection in health information systems consideration and guidelines, Amsterdam, Holland, 1980

Architecture générale d'un site



Périmètre de sécurité de l'exercice professionnel

Pilote de Rimouski :

mesures de protection exceptionnelles de type

organisationnel: périmètre de sécurité

matériel: sécurisation par carte en ligne

algorithmique: chiffrement, codification, codage, protocole

Couches de sécurité

- niveau carte à microprocesseur

- niveau SCAM (Serveur des cartes à mémoire):

  authentification par RSA

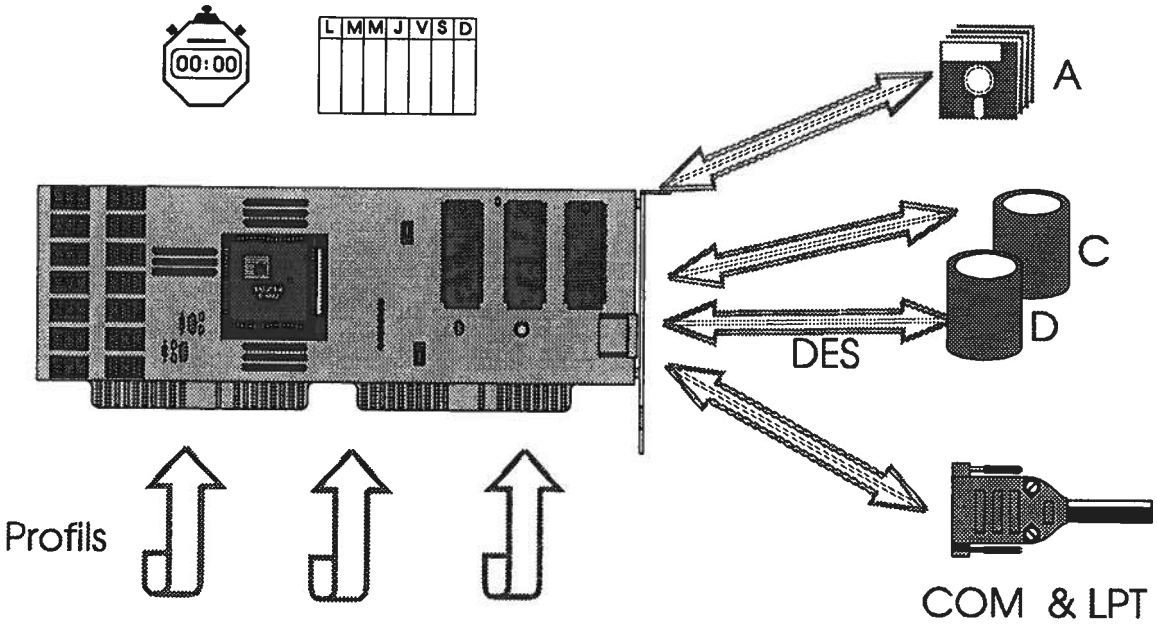
  chiffrement par DES

  codification et compaction des données

- niveau matériel par carte de sécurisation du bus et des périphériques

- niveau application: ajout facultatif de vues propres à l'application (filtres)

Sécurité par le matériel



- Contrôle les tentatives d'accès à l'ordinateur

- Gère plusieurs profils d'accès

- Restreint l'accès et le mode d'accès aux seules ressources permises (unités de stockage et lignes de communication)

- Chiffre les données sur les unités de stockage avec DES standard

- Gère le temps d'activité de l'ordinateur

Techniques d'implantation

1- intégrité des données[1]

atomicité de la transaction logique et physique: module de SCAM chargé de garantir l'atomicité logique et physique par la technique de la sentinelle sur mémoire stable (EEPROM)

2- accès sécurisé aux données de la carte

carte avec vérification interne d'un NIP pour chaque zone de données et prise en compte de la ratification (essais non fructueux)

3- communication sécurisée

usage des algorithmes de chiffrement robustes: RSA et DES

authentification des cartes par certificat

---

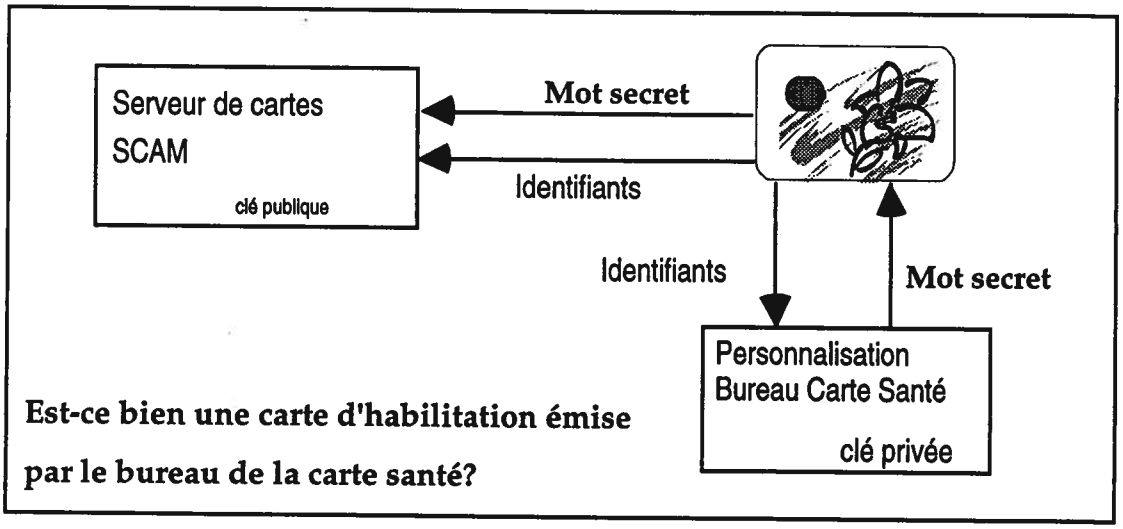
[1] Rachid Zaïane, Accès logique et compression des données de petite taille dans un dossier médical géré par carte à microprocesseur

Certification de la carte d'habilitation (CH)

algorithme RSA

principe: deux clés: l'une publique et l'autre privée

fondé sur la complexité de la factorisation des grands nombres premiers (> 90 ans pour décodage avec une puissance de calcul exceptionnelle)



numéro de série de la Carte d'habilitation

+

identifiants stockés à la personnalisation ------> mot secret placé dans la carte d'habilitation

+

clé privée de Carte Santé

Procédure d'authentification:

- lecture du mot secret de la carte d'habilitation insérée à la personnalisation

- décodage par SCAM du mot secret de la carte d'habilitation par RSA

- comparaison avec les identifiants stockés dans la carte d'habilitation

-----> si carte d'habilitation authentifiée

- lecture du NIP générique

- lecture des droits d'accès de la CH

- ouverture de la carte du bénéficiaire par le NIP

- écriture / lecture filtrée par le profil des accès par SCAM et à l'interne par la carte

Profil des accès virtuels codé par DES: modification autorisée par le bénéficiaire

Chaque carte peut autoriser une modification <u>temporaire</u> au profil d'accès de base spécifié par le bureau du projet Carte Santé

ex: autorisation de lire une zone médicale par le pharmacien avec l'autorisation préalable du porteur.

DES est un algorithme symétrique à clé secrète robuste et éprouvé

DES (profil en clair, clé secrète) = profil codé

DES^{-1} (profil codé, clé secrète) = profil en clair

Étape possible que si la carte du bénéficiaire autorise la modification du profil virtuel.

Codification et Compaction(2)

Les données sont codifiées par l'application, codées et compactées par SCAM.

Les données échangées vers la carte sont illisibles sans une table de décodification

---

(2) Rachid Zaïane et André Gamache, Correspondance entre les zones logiques et physiques du dossier de l'aide-mémoire médical, Rapport technique du Département d'informatique, LIGE, Université Laval, DIUL-RT-9201, 1992

Codage et compression des données médicales

Les applications n'écrivent pas l'information brute sur la carte mais des références à des bases de données stockées sur disque chiffré.

Pour écrire ou lire de la carte, toute application doit nécessairement transiter ses transactions par SCAM.

Par souci d'économie d'espace mémoire, SCAM codifie les données en binaire.

Chaque champ est défini par un type codé d'une façon à utiliser le moins de bits possible sur la carte.

SCAM utilise un dictionnaire de contexte contenant la structure de chaque enregistrement du dossier portable ainsi que l'association champs-types pour coder chaque information sur la carte.

Sans le dictionnaire de contexte, l'information sur la carte ne peut être interprétée.

Le dictionnaire est stocké sur une partition du disque chiffrée avec DES par la carte électronique de sécurité.

Le codage par dictionnaire de contexte permet d'allonger la durée de vie de la carte de 2,5 fois en moyenne.

Conclusions

1- **niveau de sécurité exceptionnel: accès illicite ou délictueux pratiquement impossibles et les erreurs dues à la non intégrité sont décelées.**

2- **clonage impossible des données ou du dossier médical ou de la carte d'habilitation: le clonage sera détecté par SCAM; celui de la carte santé est impraticable après personnalisation de la puce en raison de la capacité interne de traitement de la carte.**

3- **les techniques de sécurisation utilisées dans la carte santé sont transposables à d'autres technologies telle la carte à laser dont la capacité est de 4 méga octets avec une sécurité intrinsèque initiale nulle.**(3)

4- **La sécurisation des données permet d'accroître la capacité effective de la mémoire : 8 k octets sur carte pour 20 k octets traités par une application.**

Remerciements

Le travail de conception et de réalisation est celui d'une équipe du LIGE à laquelle ont participé R. Zaïane, G. Girard, P. Durant, H. Guibert, E. Bellavance, P. Ardouin et A. Gamache.

* * *

(3) [1]H. Guibert , Etude de faisabilité du dossier médical portable sur carte à mémoire optique, Rapport technique du Département d'informatique, LIGE, Université Laval, DIUL-RR-9301, 1993