



Data Protection 2.0

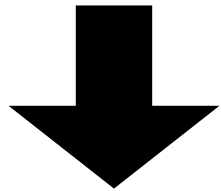
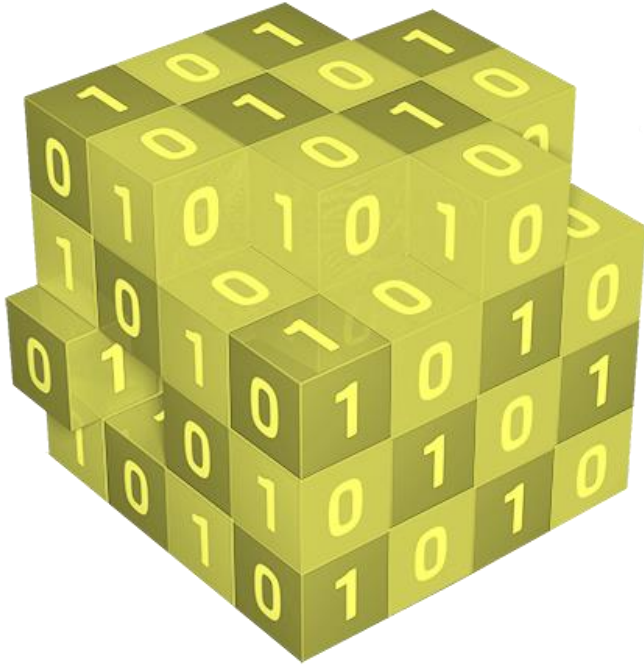
Tania Martin

Smals Research

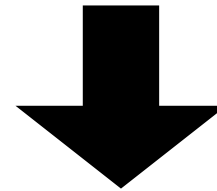
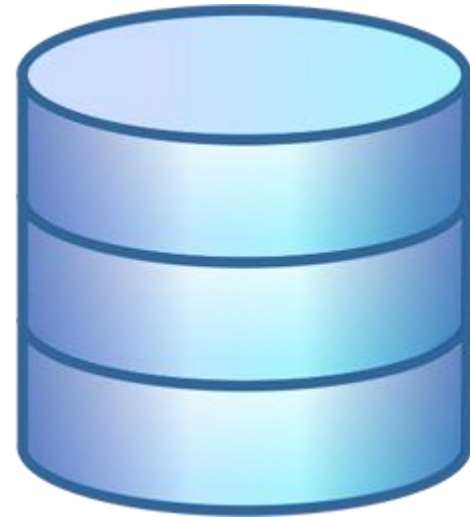
www.smalsresearch.be

Juin 2016

Symboles de la présentation



Données



Base de données

Contexte

 **sensibles**

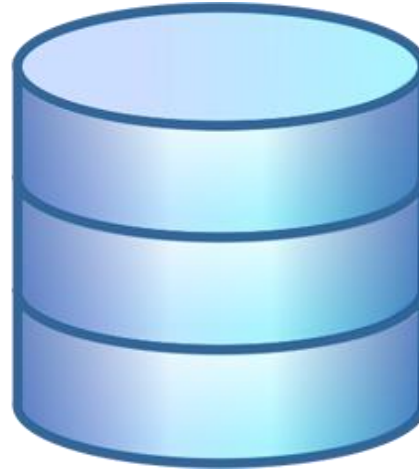


HR

+

00 00 00 00 00

Beaucoup de 



Accessibilité



User

Business analyst

Data scientist

Hacker

DBA/sysadmin

Bad user

Pourquoi faut-il protéger les des ?



Recherche scientifique



Testing d'application



Partage entre institutions



Quels types de ?



Smals

70% Oracle

10% MySQL

10% MS SQL

10% Adabase

PostgreSQL (futur)



Membres

Oracle

MySQL

MS SQL

IBM DB2

Agenda

1

Les murs, protection traditionnelle

2

Data-centric security model

Principes du modèle

Où s'applique le modèle

3

Produits intéressants

4

Recommandations

Les murs, protection traditionnelle



Quels types de murs ?

Murs physiques

Contrôle d'accès

Firewalls

Outils de DLP

Etc.



**Défenses
périphériques**

Chaque mur rajoute...

Protection
ad-hoc


Complexité

Coûts

Surcharge dans
le système



Et l'on constate que...

“En 2016, plus de 80% des entreprises ne parviendront pas à développer une politique de sécurité des  consolidée à travers les silos.

Cela conduira à des potentielles non conformités, failles de sécurité, et dettes financières.”

selon **Gartner**[®]

Les murs ne sont pas impénétrables

Attaquant externe

- Social eng.
- 0-day exploit

Attaquant insider

- Malveillant
- Gaffeur

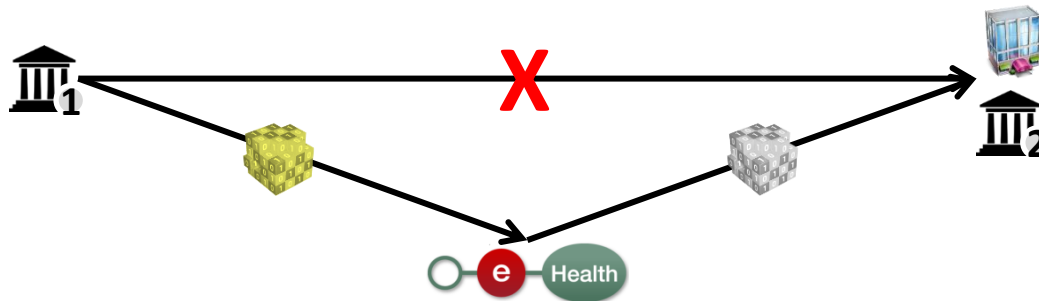


**NE PAS sous-estimer
NI ces adversaires
NI leur potentielle action**

Il existe des protections pour



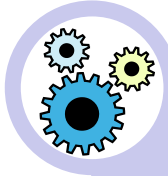
Service "Codage, anonymisation et TTP"



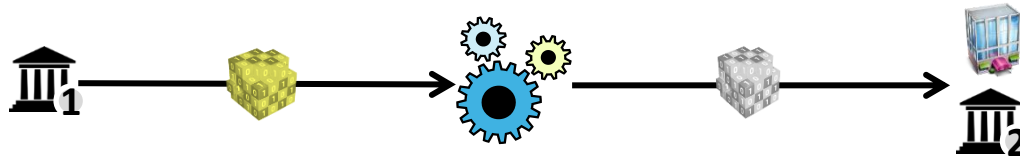
Crypto forte
(AES-CCM)

Anonymisation
du NISS
seulement

Il existe des protections pour



ARX / Argus / Camouflage / etc.



Transformations
à sens unique

Utilisation
+ ou - manuelle

Il existe des protections pour

Protect DB

DB Protector



DB Guardian

Outils DB
spécifiques

Aujourd'hui, harmonisation incertaine

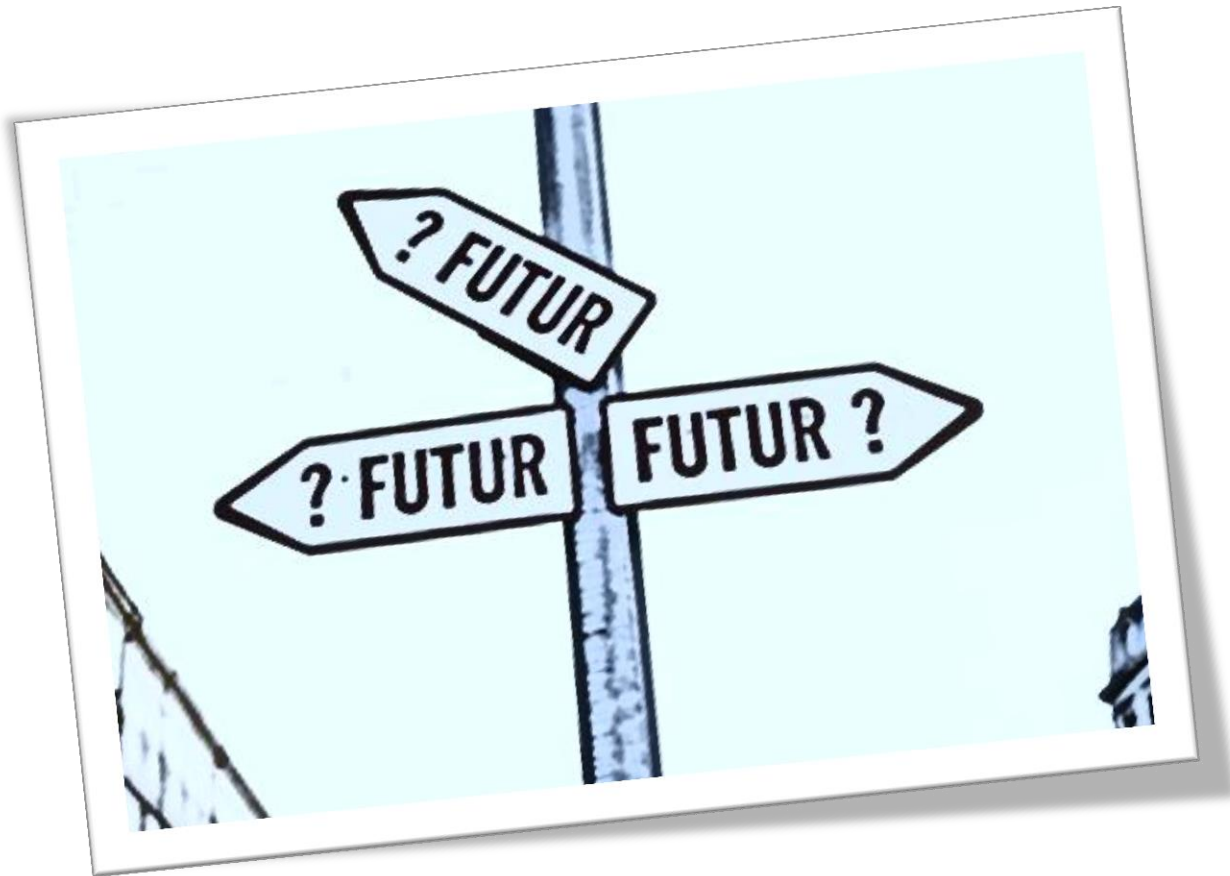
Protect DB

DB Protector



DB Guardian

Outils DB
spécifiques






Data-centric security model


C'est quoi?

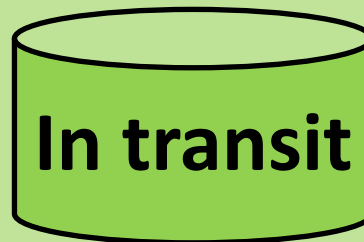
DEFINITION

Fournir une console de gestion unique qui permet l'application d'une politique de sécurité des  dans des formats de stockage de données multiples

C'est quoi?



Protéger toute  définie comme
sensible partout et à tout moment
dès qu'elle est introduite dans le
système



Principes du modèle

- 1 Data Classification & Discovery
- 2 Centralized Security Policy Management
- 3 Monitoring of User Privileges and Activity
- 4 Auditing and Reporting
- 5 Event Detection, Analysis and Alerting
- 6 Fine Grained Data Protection

1

Data Classification & Discovery

Classification = base de la sécurité




sensible?

Quel niveau
de sensibilité?

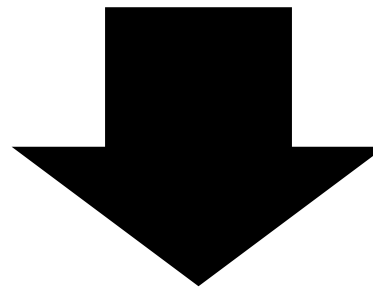
Lieux de
stockage?

Qui a
accès?

Dans quelles
circonstances?

Risques si 
compromise?

Localement
ou à
l'extérieur?



Data prioritization

Pas gravé dans la pierre!



pas statiques

Classification
pas statique

EX

Une application demande + d'infos qu'avant (ex. année à date de naissance)

→  change et devient ***sensible***


EX

Un doc Word avec NISS doit être classifié ***sensible***

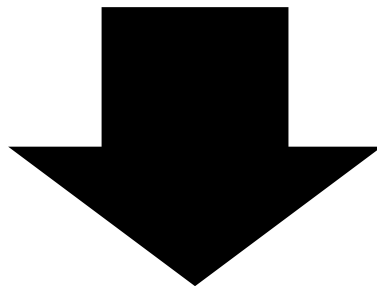
→ Si NISS enlevé du doc, alors classification plus d'application


Le point de vue de l'attaquant



Il n'y a que 2 types de  existantes dans toute organisation:

1. Celles que je veux voler
2. Les autres



Comprendre/connaitre les  est le + important

Tips pour classifier (1)

Automatiser avec l'aide d'un dictionnaire

Classifier  par contexte ou contenu

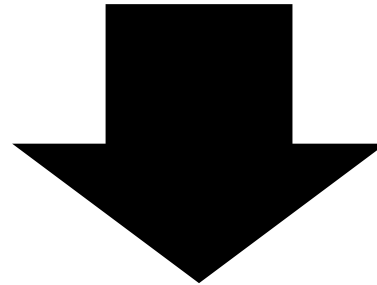
Voir si  cherchée dans BLOB

Si  chiffrée, recherche difficile

Tips pour classifier (2)


Appliquer des « tags » aux 


Utiliser des « pop-up » de mise en garde



**Self security awareness
in real time**

Exemple de classification

 Classification	
Nom	Sensible
NISS	
Date de naissance	
Adresse	
Salaire	Non-sensible
Religion	
Hobbies	

 Cet exemple de classification n'est pas valide dans tous les cas de figure.

2

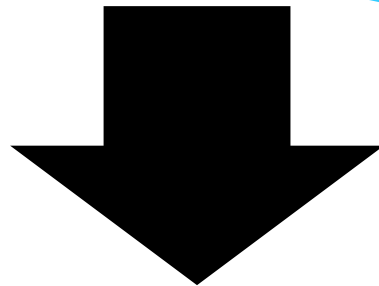
Centralized Security Policy Management

Classifier 1 fois, appliquer partout

Consistence de la protection des



Protection/silo
=
trous de management
et de contrôle



Politique centralisée
doit être appliquée à
chaque  **dans chaque silo**

Définition des utilisateurs

Coordination
des rôles et
responsabilités

Utilisation de
LDAP/AD pour auth
des identités et rôles

Segregation
of duties

EX

Pour un DB change:

• Change request =



Analyst

• Authorisation & approval =



Manager

• Design & dev =



Developer

• Review =



Developer

• DB change =



DBA

Tips pour la politique centralisée



Bien connaître les employés et leurs accès

Limiter les erreurs sur le contrôle d'accès

Une seule console de gestion

3

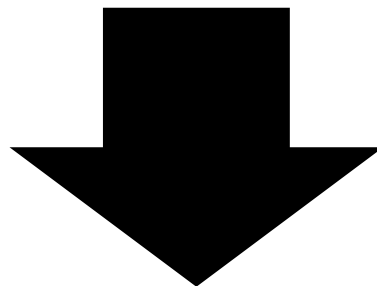
Monitoring of User Privileges and Activity




aux changements dans LDAP/AD

Nouveaux
utilisateurs?

Nouveaux
privilèges
individuels?



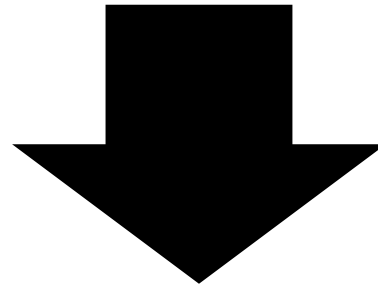
Match avec requirements du
business rôle, type de  et
localisation géographique



aux changements de privilèges

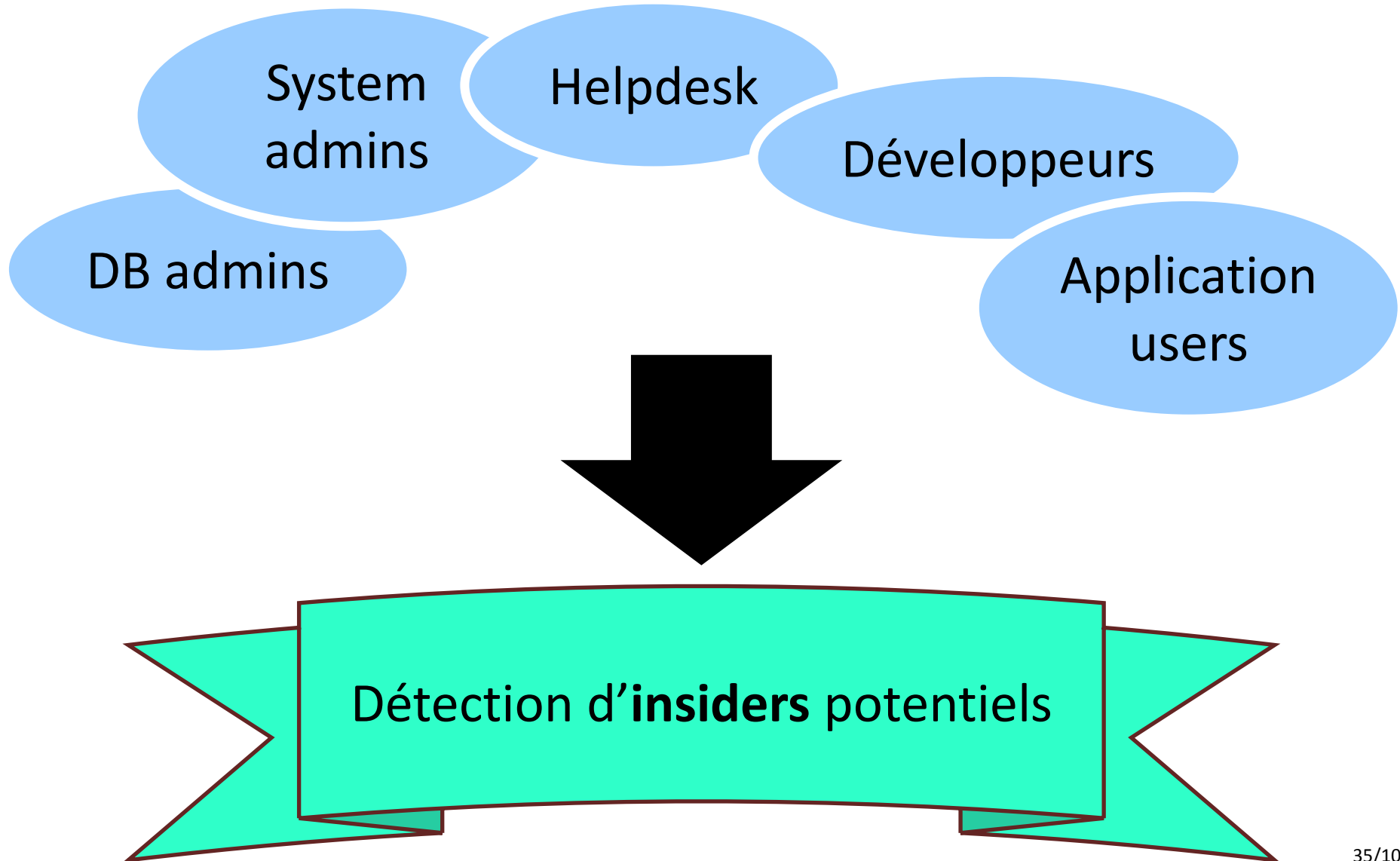
Escalations
de
privilèges?

Changements
de privilèges
sur des  ?



Détection d'**insiders** ou **hackers**
externes potentiels

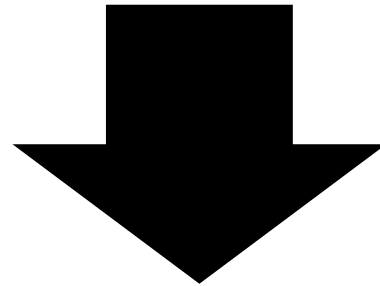
Privileged user monitoring



Database activity monitoring

Analyse de
toutes les
requêtes SQL

In real
time



Détection d'**insiders** ou **hackers**
externes potentiels

Tips pour le monitoring



Monitoring en continu

Même lors de pics d'utilisations

Même lors de congestions réseau

Même en cas de latence

4

Auditing and Reporting


Le point de vue de l'auditeur

J'ai besoin de
connaître de
façon approfondie
l'activité des users



Pistes d'audit

Comportements
inhabituels des users

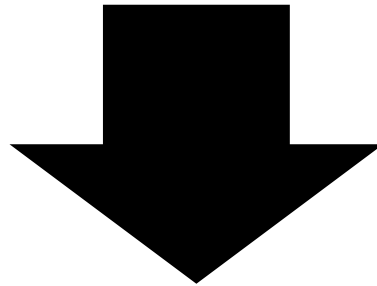
Changements
des 

Violation de la
politique

Changements
de privilèges

Importance en cas d'incident

Se baser sur
les logs d'audit

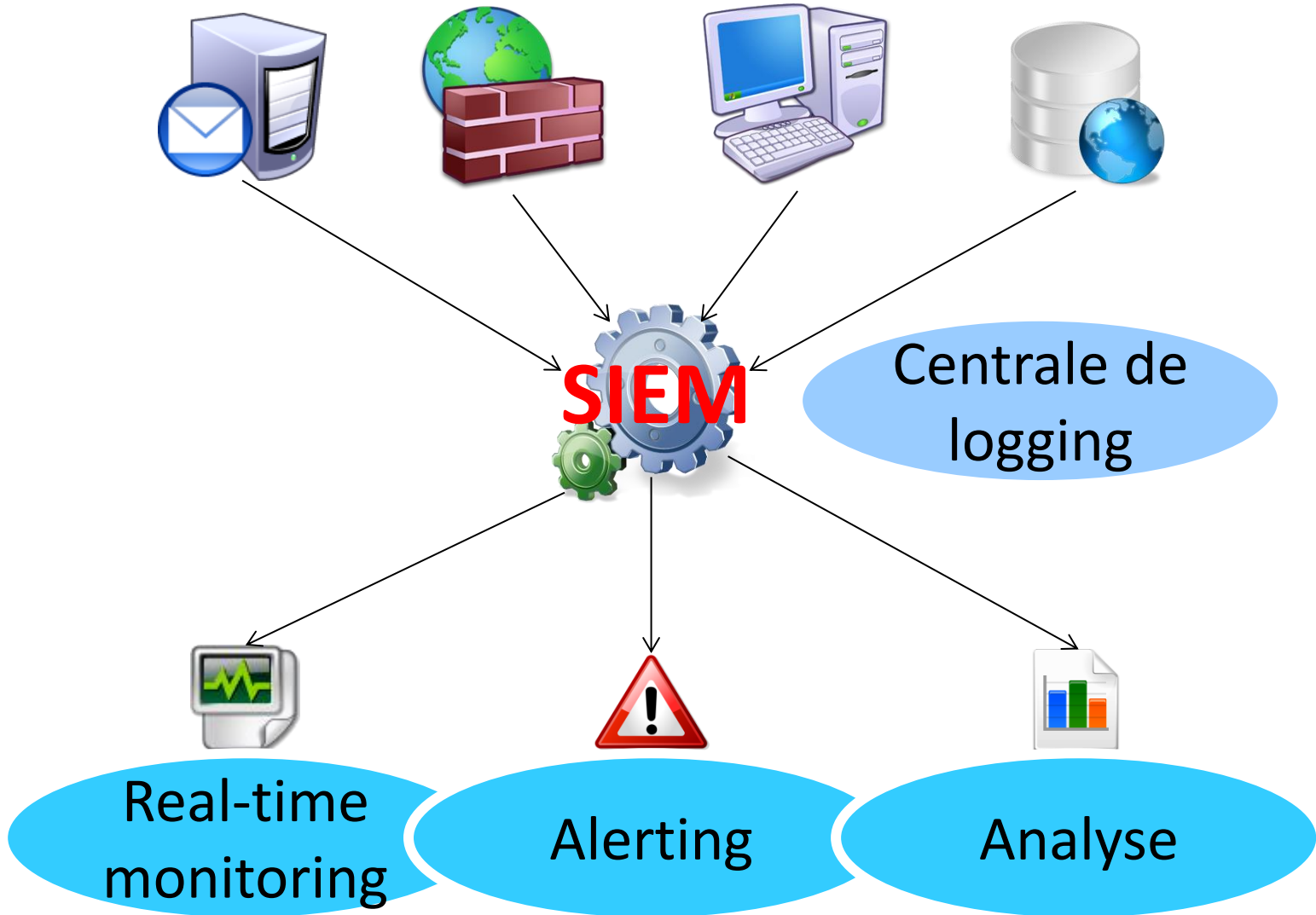


Analyse forensic pour enquêter
sur les activités étranges

5

Event Detection, Analysis and Alerting


Création d'alertes indispensable



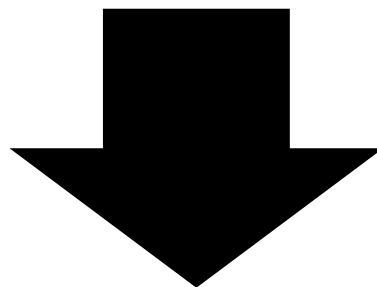
Mesures + ou - radicales

Bloquer
automatiquement
certaines actions

Délivrance
de privilège

Fermeture de
tout accès à
une 

Suppression
de privilège



Granularité des alertes, du
reporting et des mesures

Pause



Agenda

1

Les murs, protection traditionnelle

2

Data-centric security model

Principes du modèle

Où s'applique le modèle



3

Produits intéressants

4

Recommandations


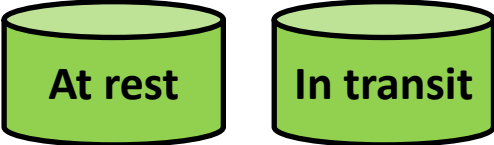
6

Fine Grained Data Protection

Granularité de la protection


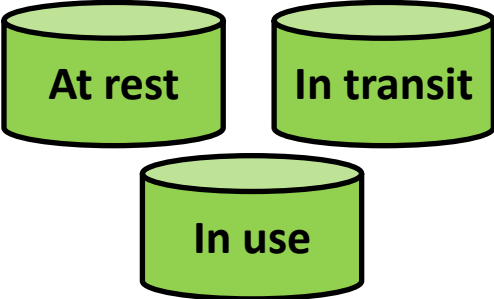


Coarse Grained

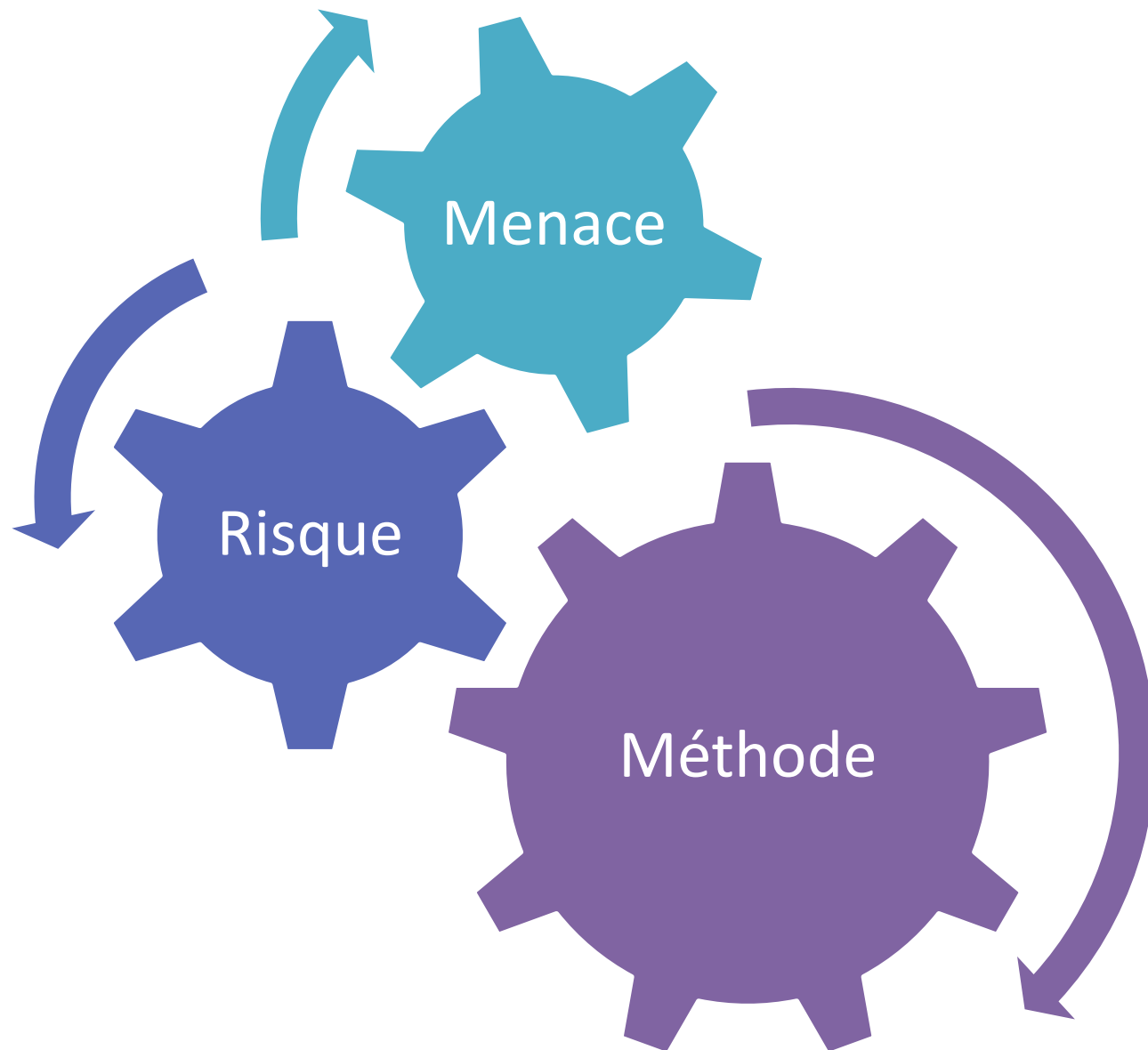
- ▶ Niveau *volume/fichier*
- ▶ Tout ou rien
- ▶ Pas sécurisation 
- ▶ Sécurisation 



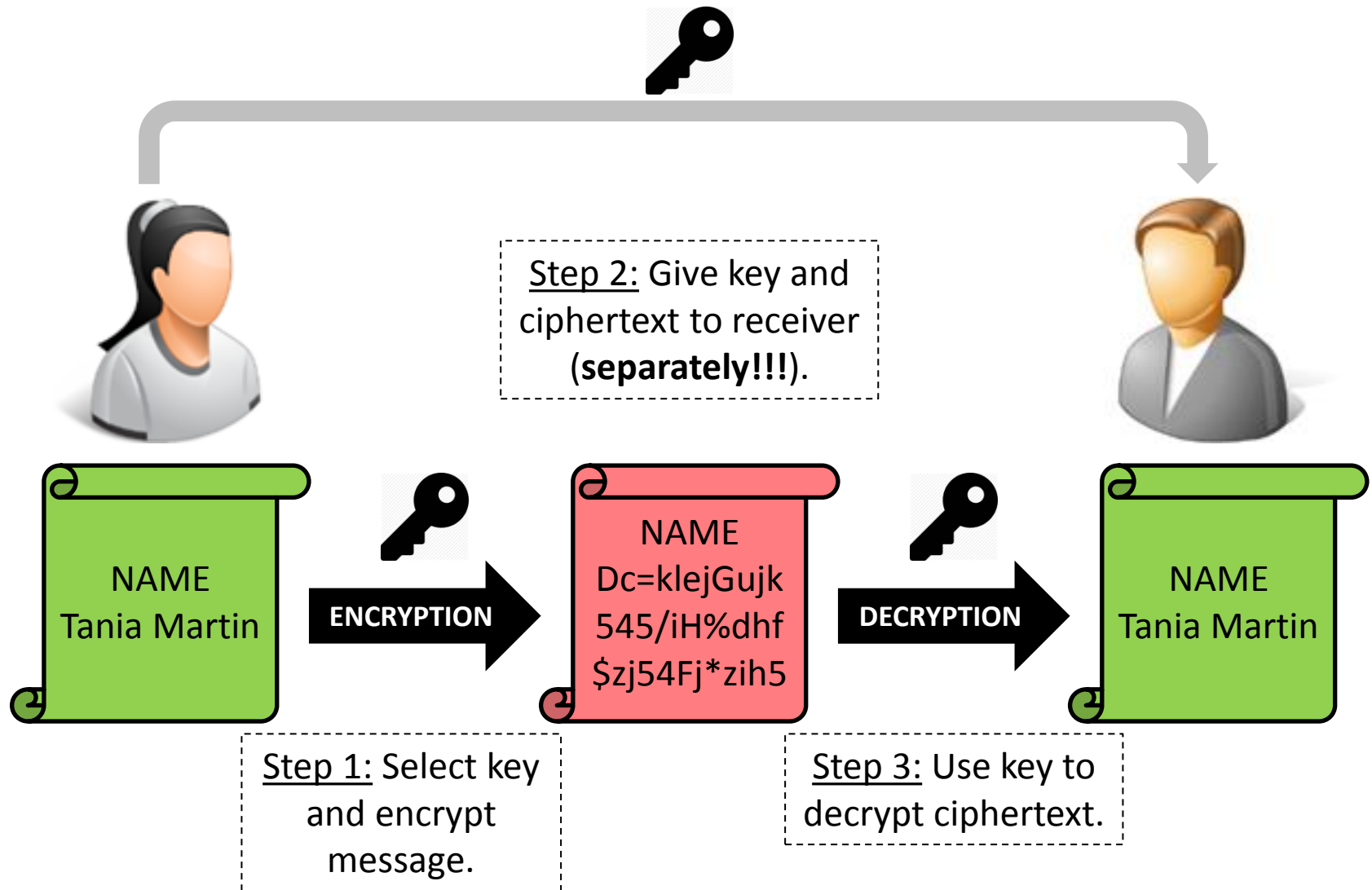
Fine Grained

- ▶ Niveau */champ*
- ▶ Plusieurs méthodes
- ▶ Sécurisation 

Quid: méthode vs. type de protection



Chiffrement classique



Chiffrement classique

Réversible

No
sort

No
search

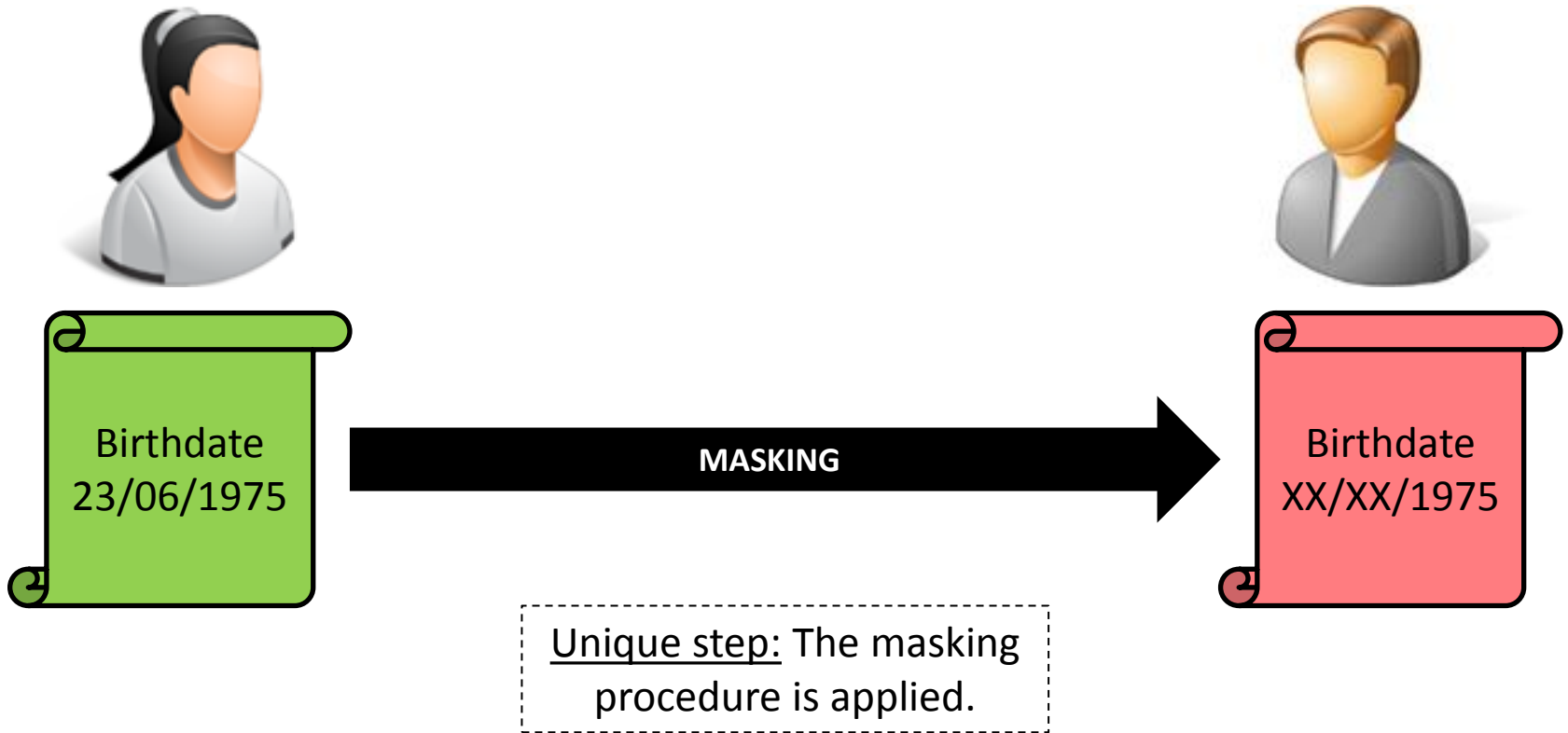
Gestion des
compliquée


non-utilisables

Pas forcément
la meilleure méthode



Masking





Masking

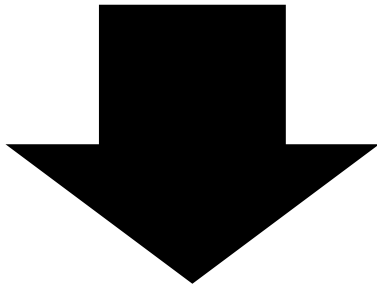
Pas réversible

Partial
sort

Partial
search

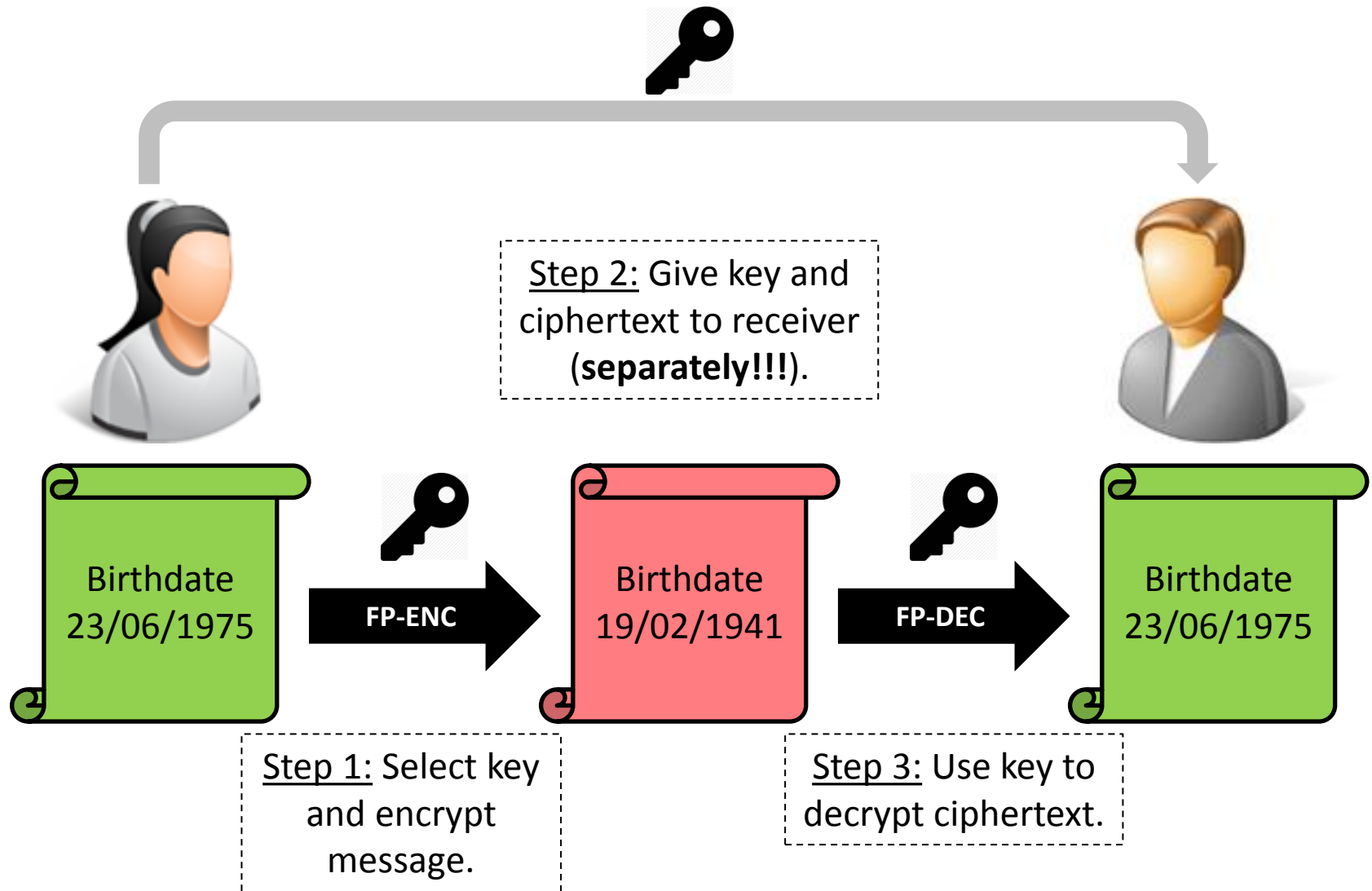
Pas de gestion
de 


semi-utilisables



Pas forcément
la meilleure méthode

Format preserving encryption (FPE)



Format preserving encryption (FPE)

Réversible

Possible
sort

Possible
search

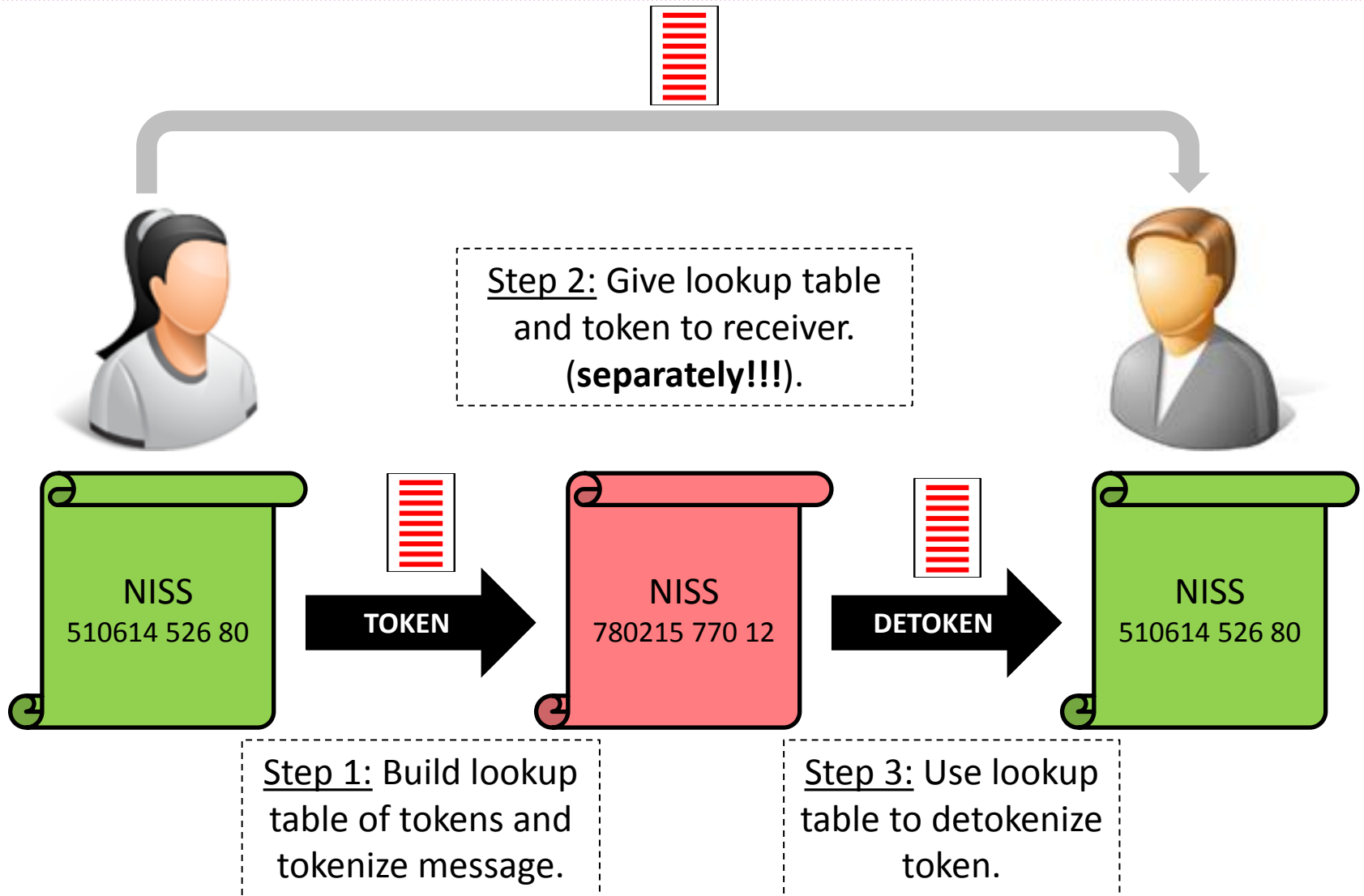
Gestion des
compliquée

utilisables *as-is*

Assez bonne méthode

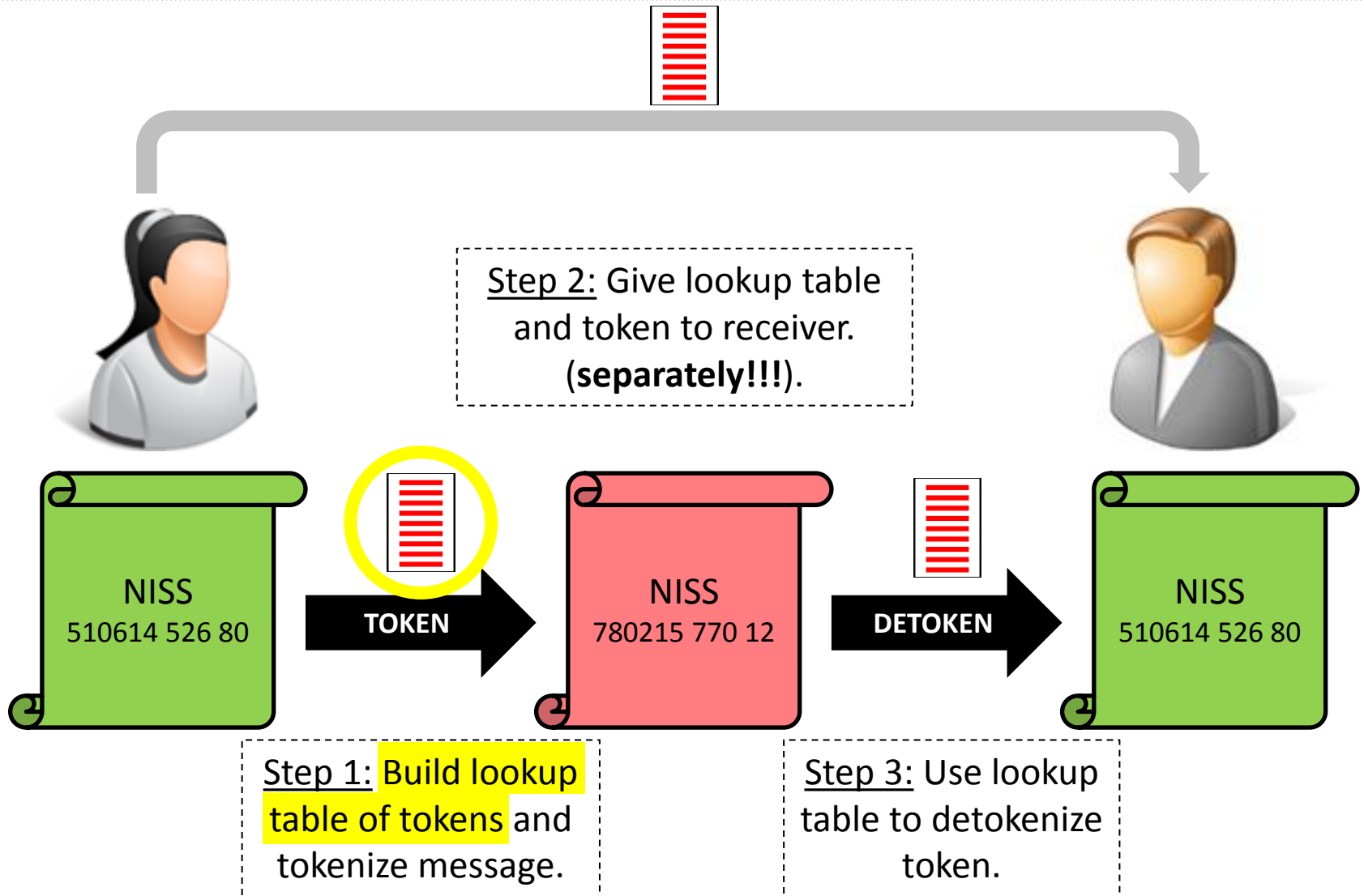


Tokenization





Tokenization






Tokenization

1

Vault-based tokenization

- ▶ Mapping random unique
Original ↔ *Token*
- ▶ Zéro relation mathématique
- ▶  grossit dynamiquement


NISS	
Original	Token
510614 526 80	↔ 7802515 770 12
210705 483 36	↔ 021501 294 56
110110 945 40	↔ 125615 973 19
491208 212 56	↔ 425878 775 54
921123 488 41	↔ 115465 841 65
970309 474 71	↔ 054648 220 07
850215 256 26	↔ 585565 893 24
750830 021 19	↔ 562589 542 01
	•
	•
	•



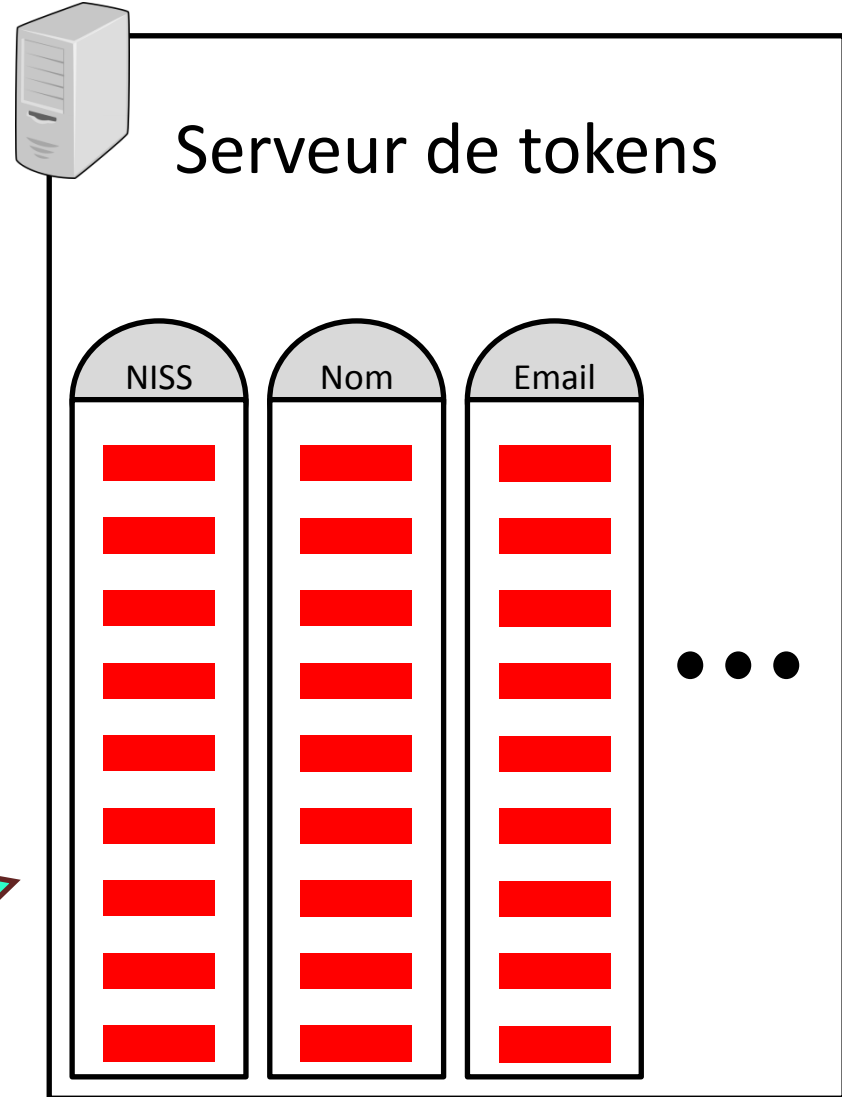
Tokenization

1

Vault-based tokenization

- ▶  ne font que grossir
- ▶ Réplications deviennent plus complexes

Solution pas gérable

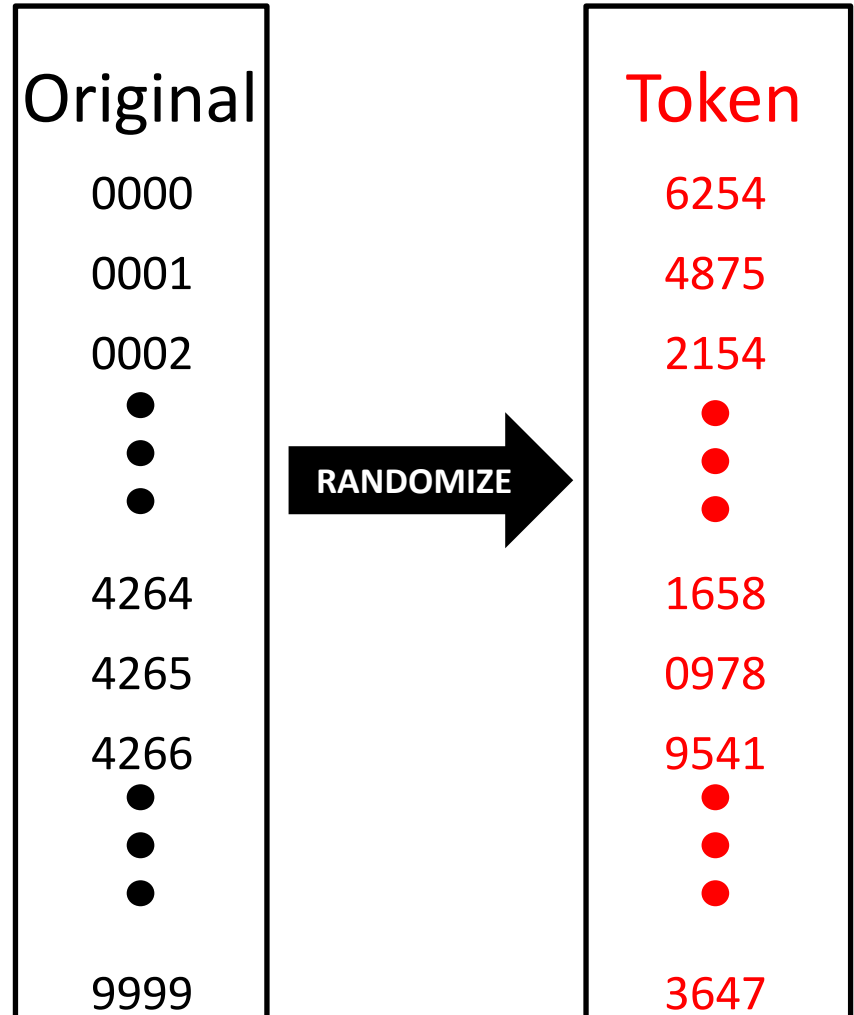




Tokenization

2

Vaultless tokenization










Tokenization

2

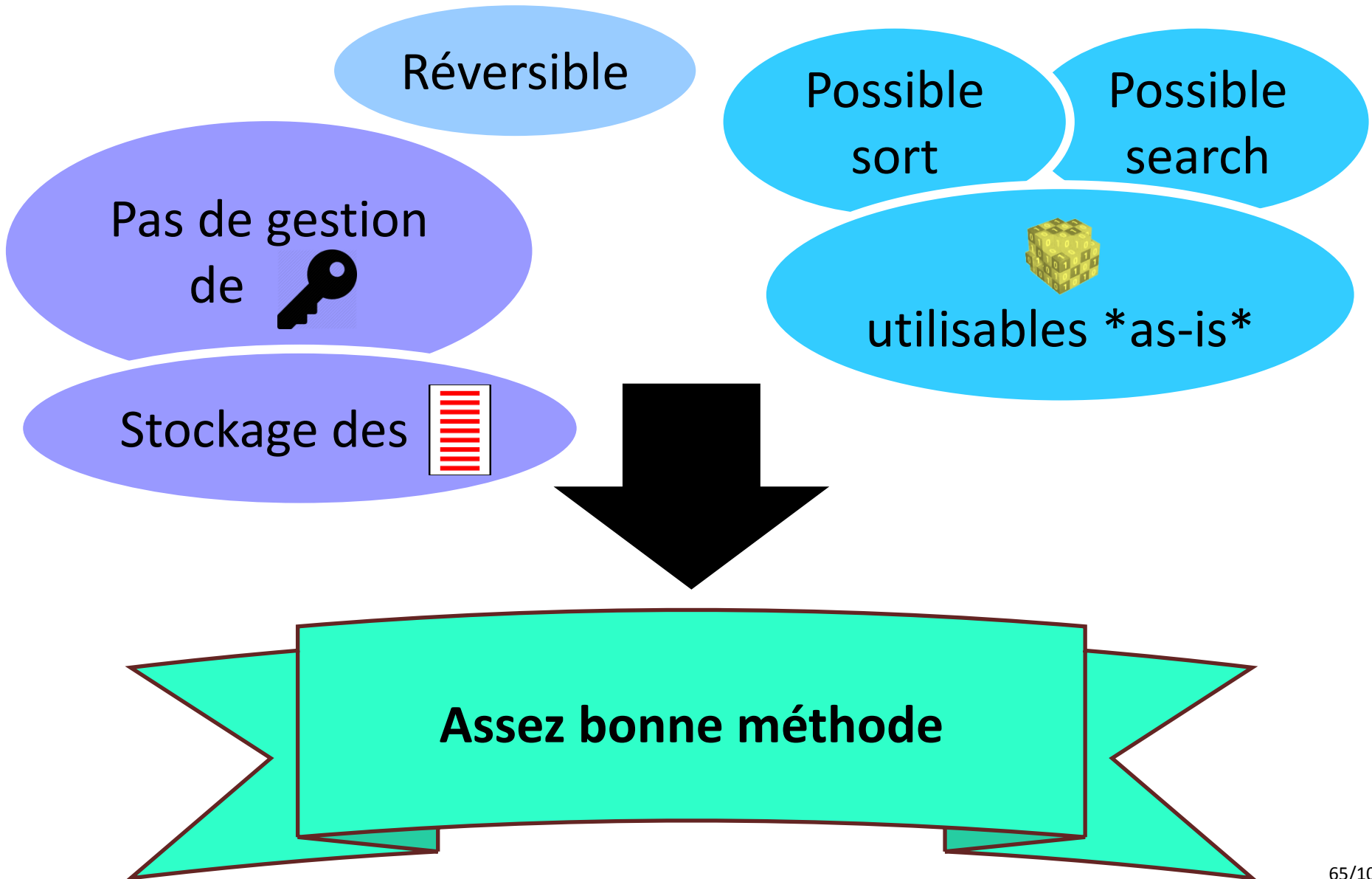
Vaultless tokenization

- ▶ 1 ou plusieurs  /  type
- ▶  randomisée
- ▶  pré-calculée
- ▶  plus petite

Origin	Token
0000	6254
0001	4875
0002	2154
●	●
●	●
●	●
4264	1658
4265	0978
4266	9541
●	●
●	●
●	●
9999	3647




Tokenization



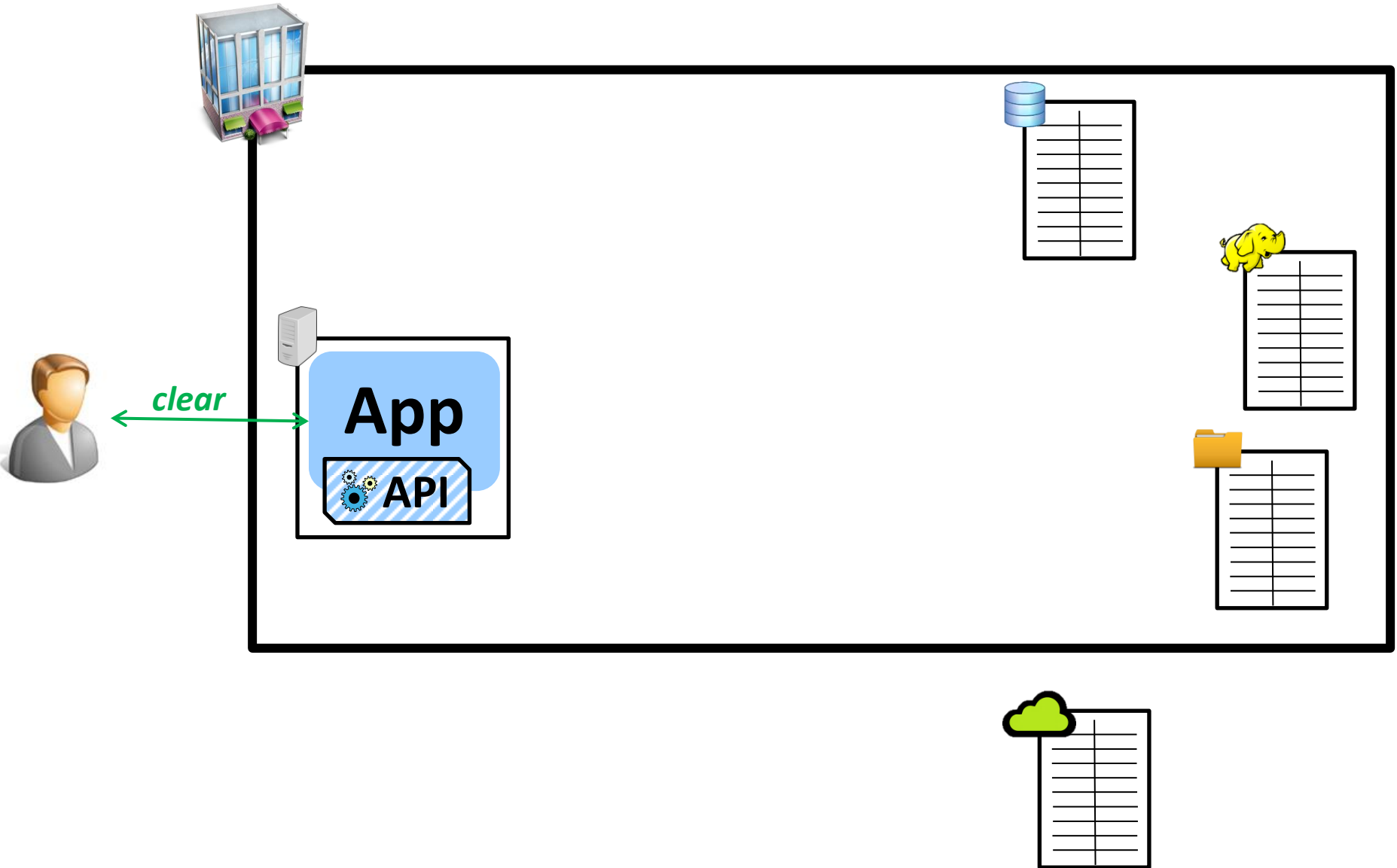


Tokenization

	Clear	Tokenized
Nom	Jan Dupont	cZu TusLPf
Adresse	100 rue Neuve, 1040, Bruxelles-Capitale	548 Xrk maYHq, 3549, Bruxelles-Capitale
Date	23/06/1975	19/02/1975
NISS	750623-556-03	620527-039-20
Carte crédit	3678 2289 3907 3378	9846 4290 9371 3378
Téléphone	0475 01 02 03	0488 64 38 27

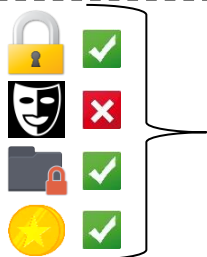
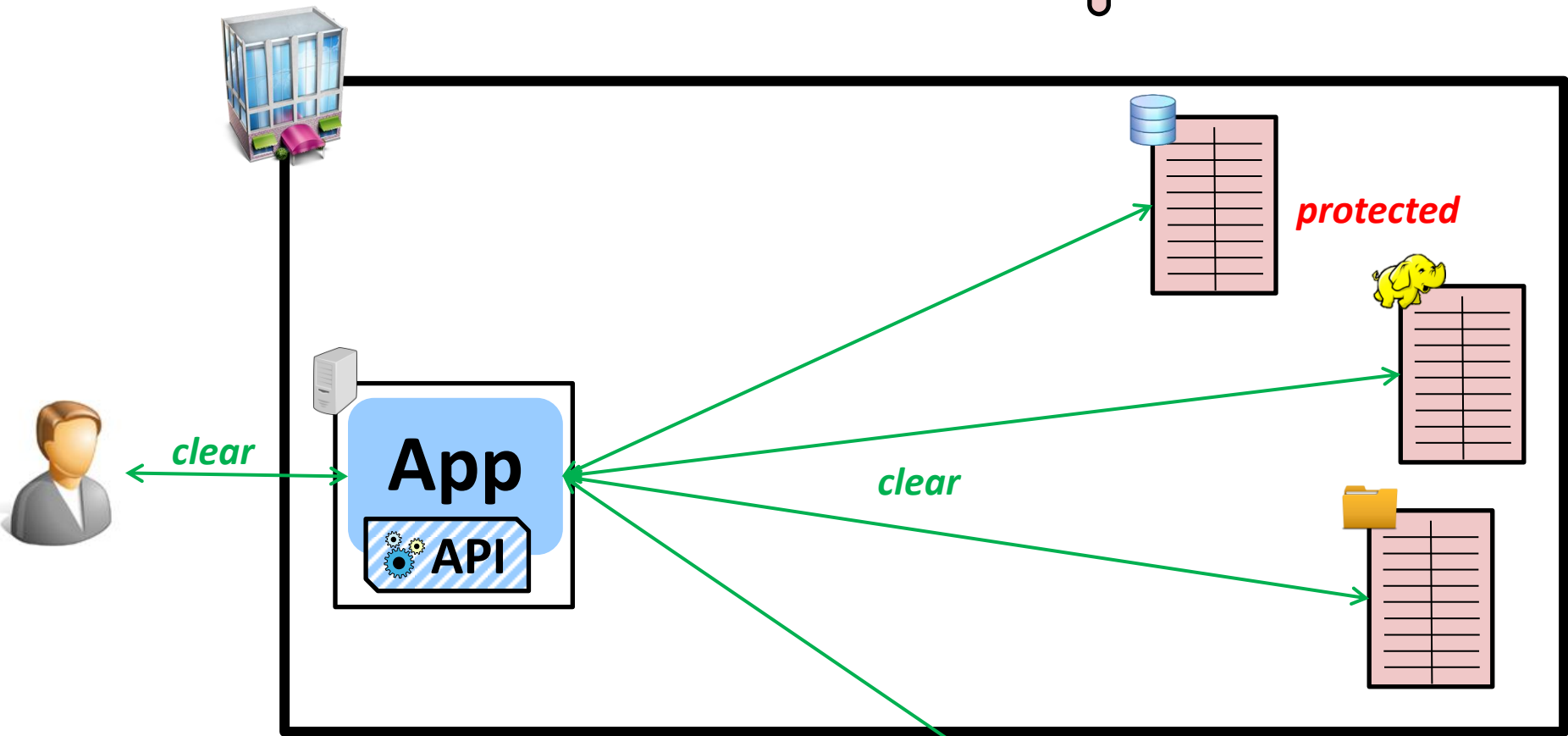
 Cet exemple de tokenization n'est pas unique.

Où s'applique la méthode?



Où s'applique la méthode?

Stockage

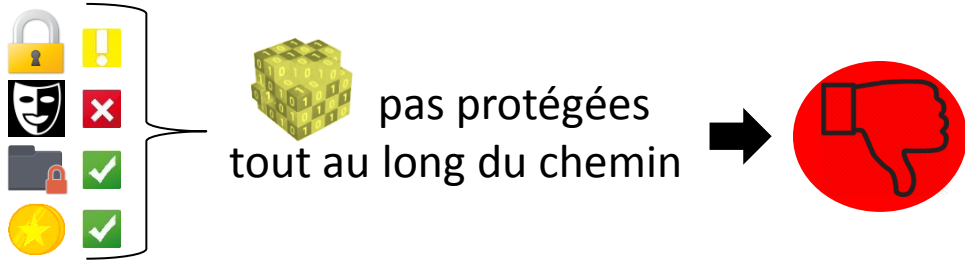
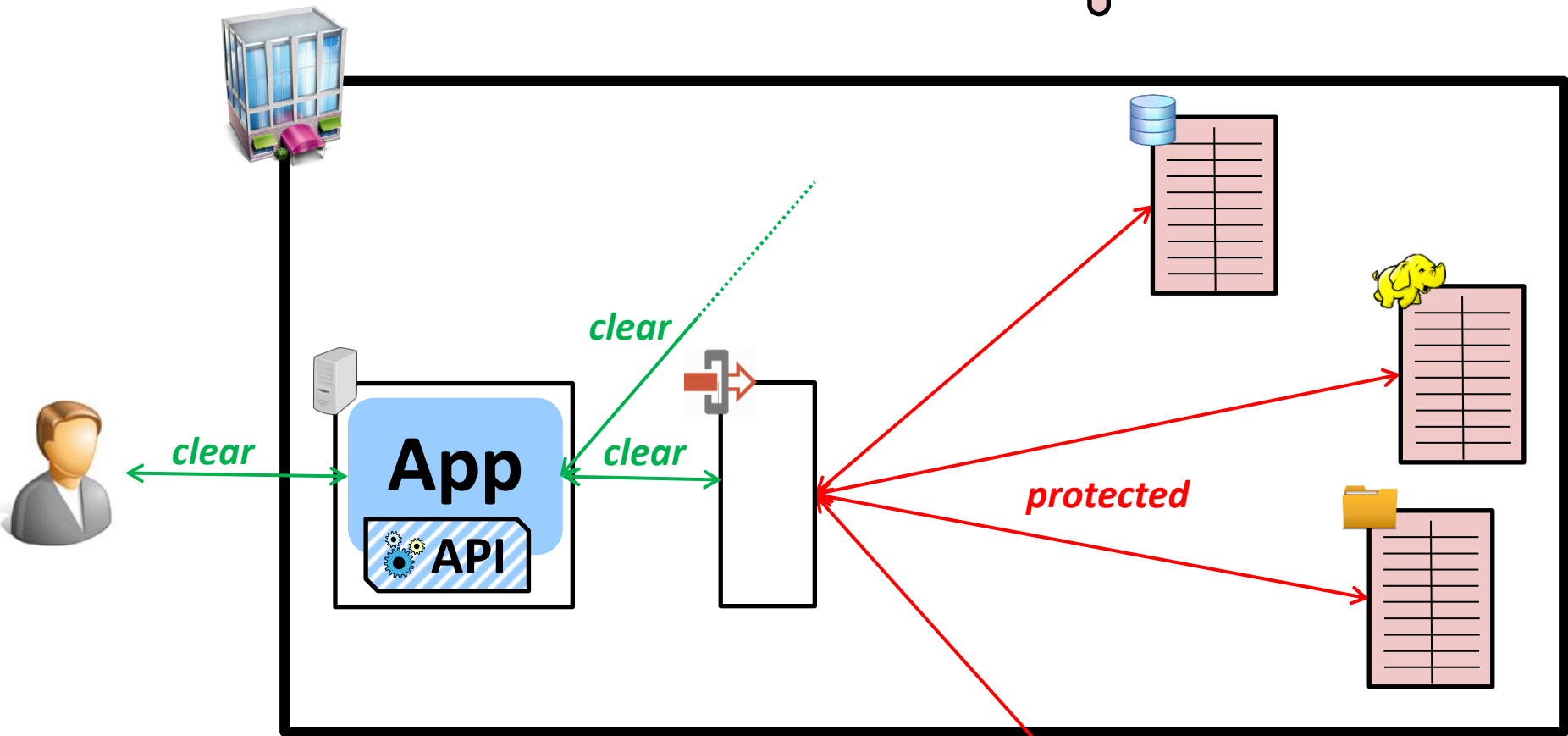


Sysadmin a
accès aux

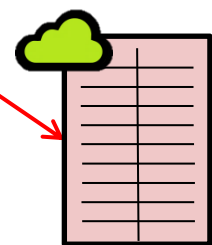
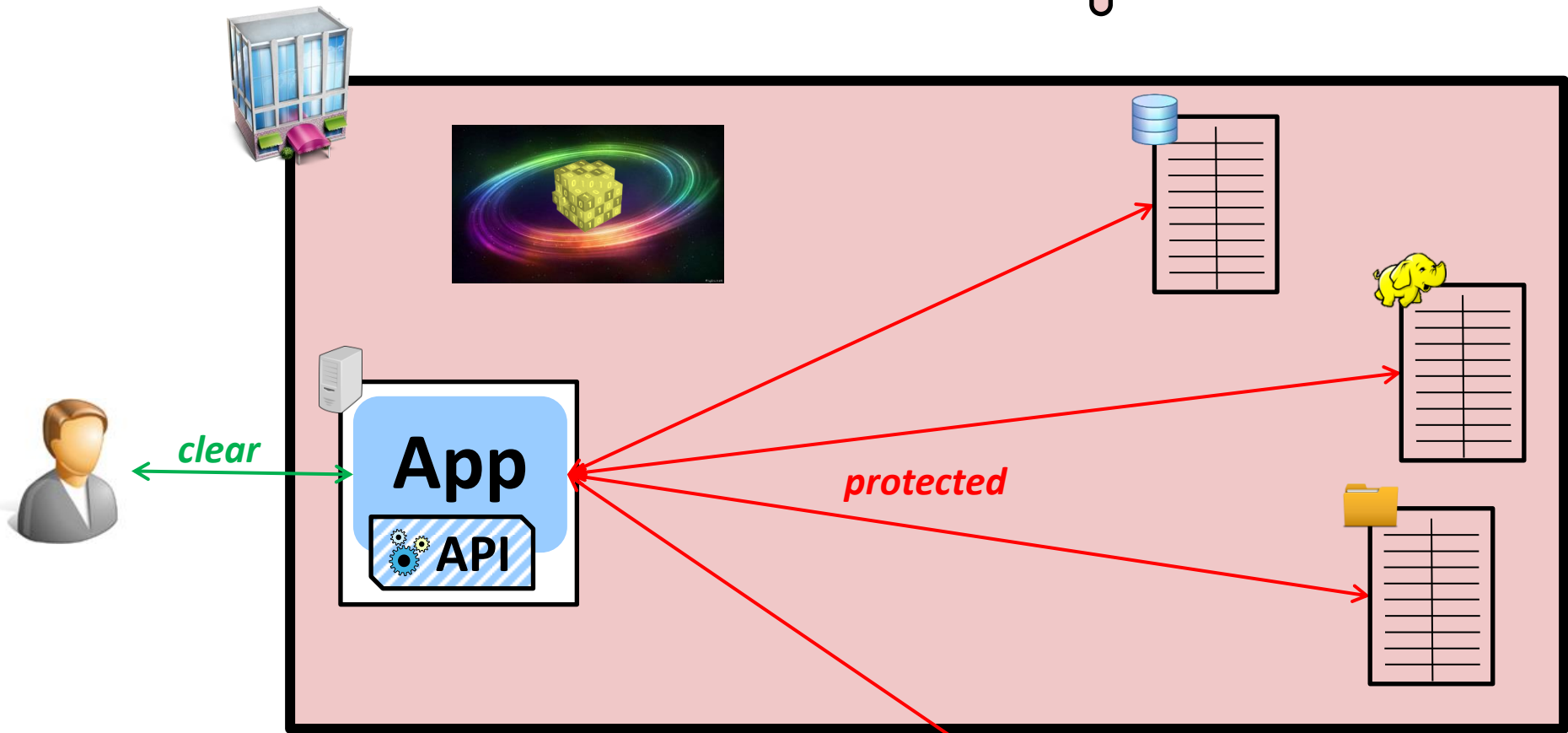
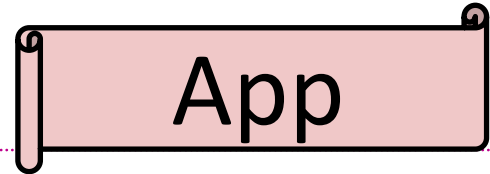


Où s'applique la méthode?

Gateway

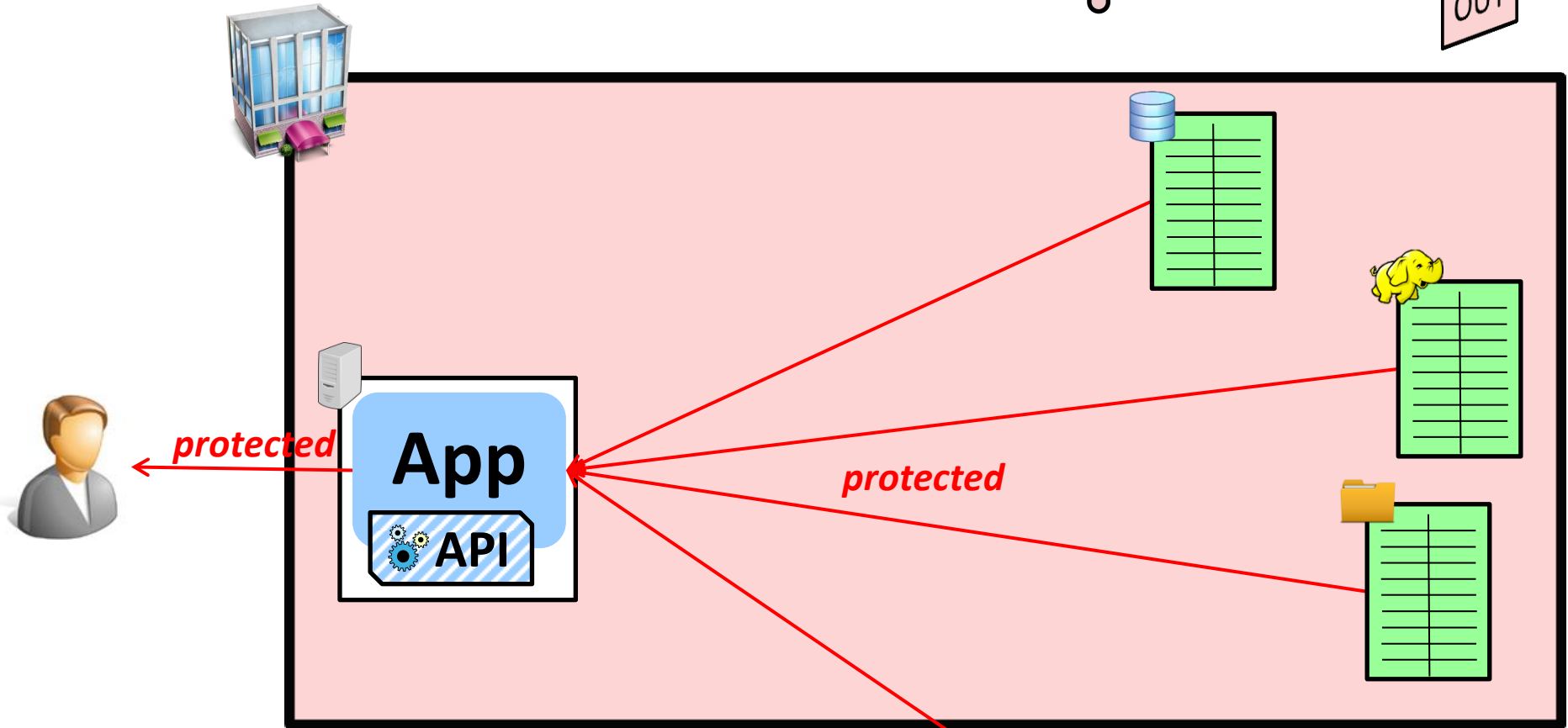




Où s'applique la méthode?



Où s'applique la méthode?




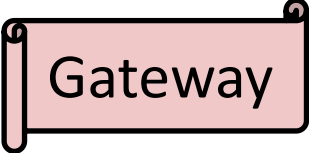


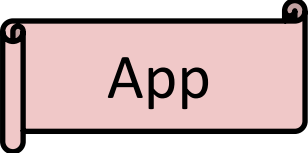



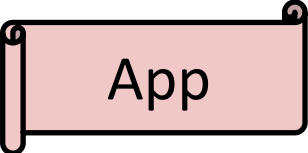



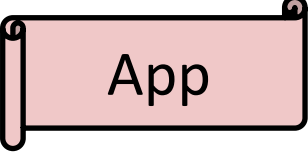



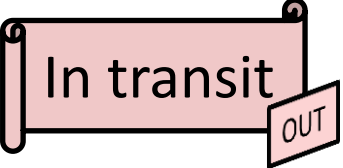




In transit
OUT






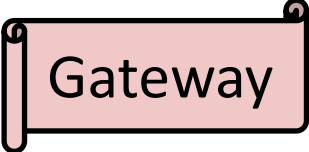


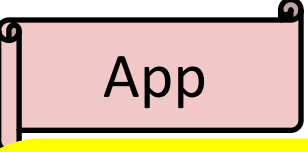



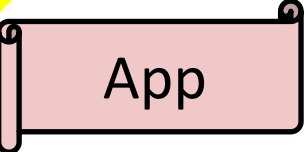



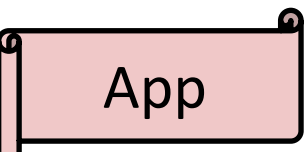



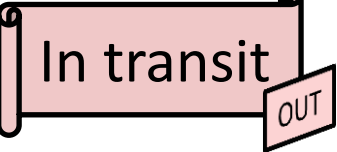



DBA et sysadmin ont accès aux  

Legend:
- Lock icon: (Red X)
- Mask icon: (Green checkmark)
- Server rack icon: (Red X)
- Star icon: (Red X)

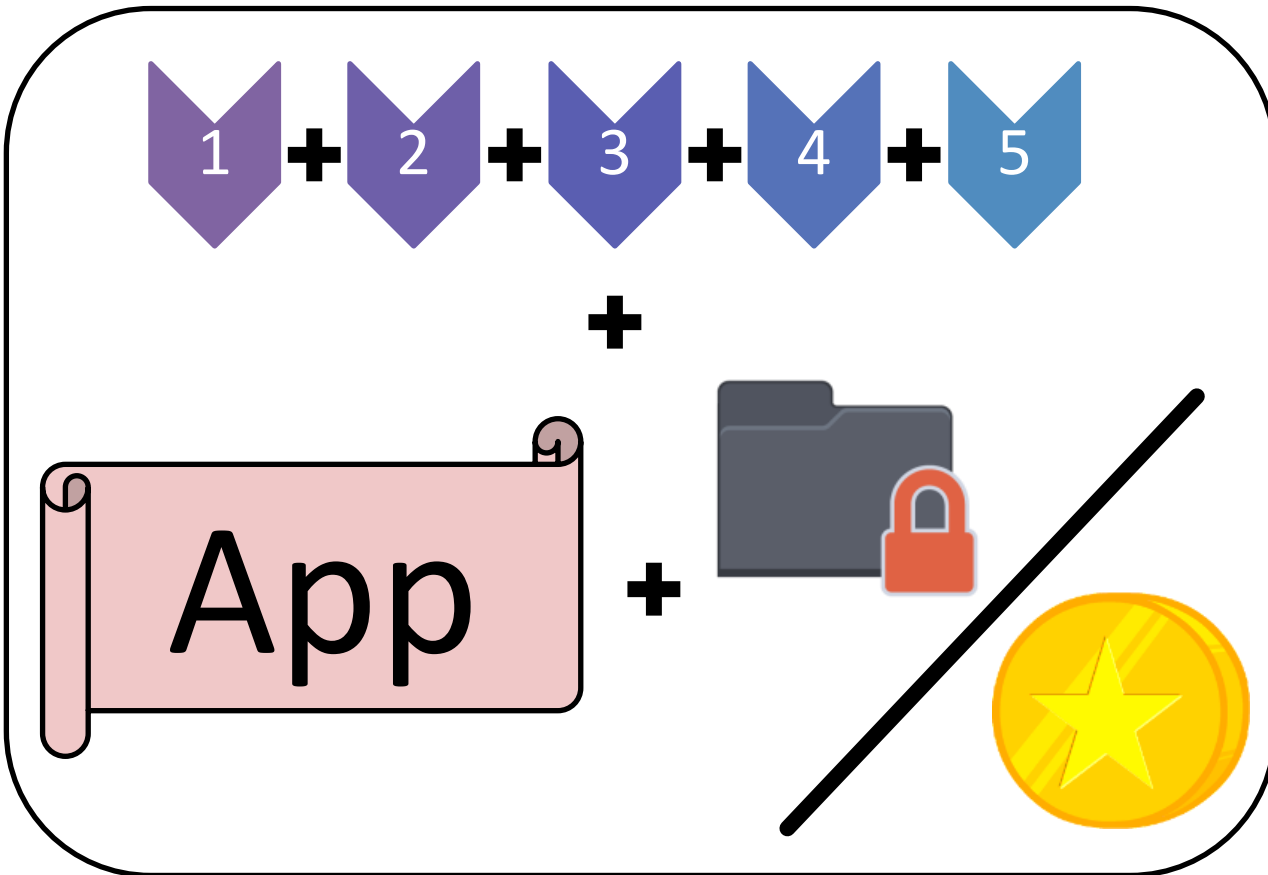
Comparatif des méthodes

 Stockage	=	Sysadmin a accès aux 	➔		
 Gateway	=	 pas protégées tout au long du chemin	➔		
 App	+	 =	Déchiffrement obligatoire pour utiliser les 	➔	
 App	+	 =	 protégées tout au long du chemin	➔	
 App	+	 =	 protégées tout au long du chemin	➔	
 In transit 	+	 =	DBA et sysadmin ont accès aux 	➔	

Comparatif des méthodes

	=	Sysadmin a accès aux 	→	
	=	 pas protégées tout au long du chemin	→	
 + 	=	Déchiffrement obligatoire pour utiliser les 	→	
 + 	=	 protégées tout au long du chemin	→	
 + 	=	 protégées tout au long du chemin	→	
 + 	=	DBA et sysadmin ont accès aux 	→	

A retenir





Produits intéressants

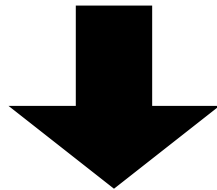
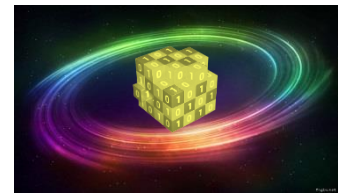
Produits intéressants



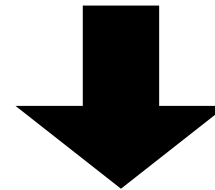
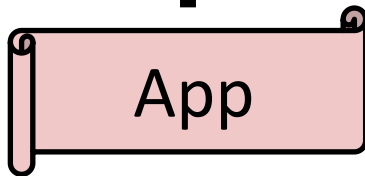
Produits intéressants



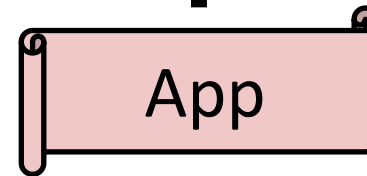
Produits intéressants pour



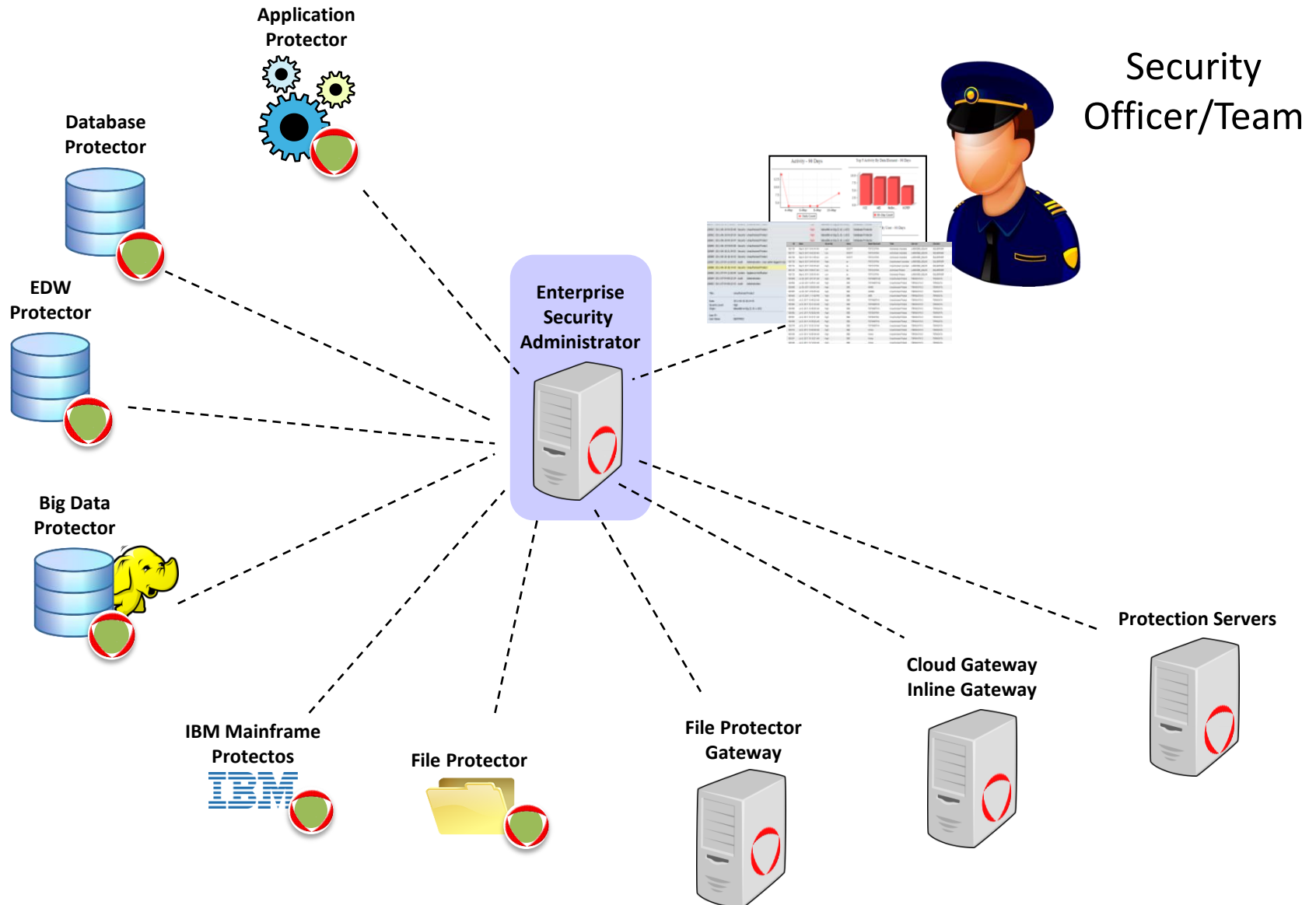
+



+



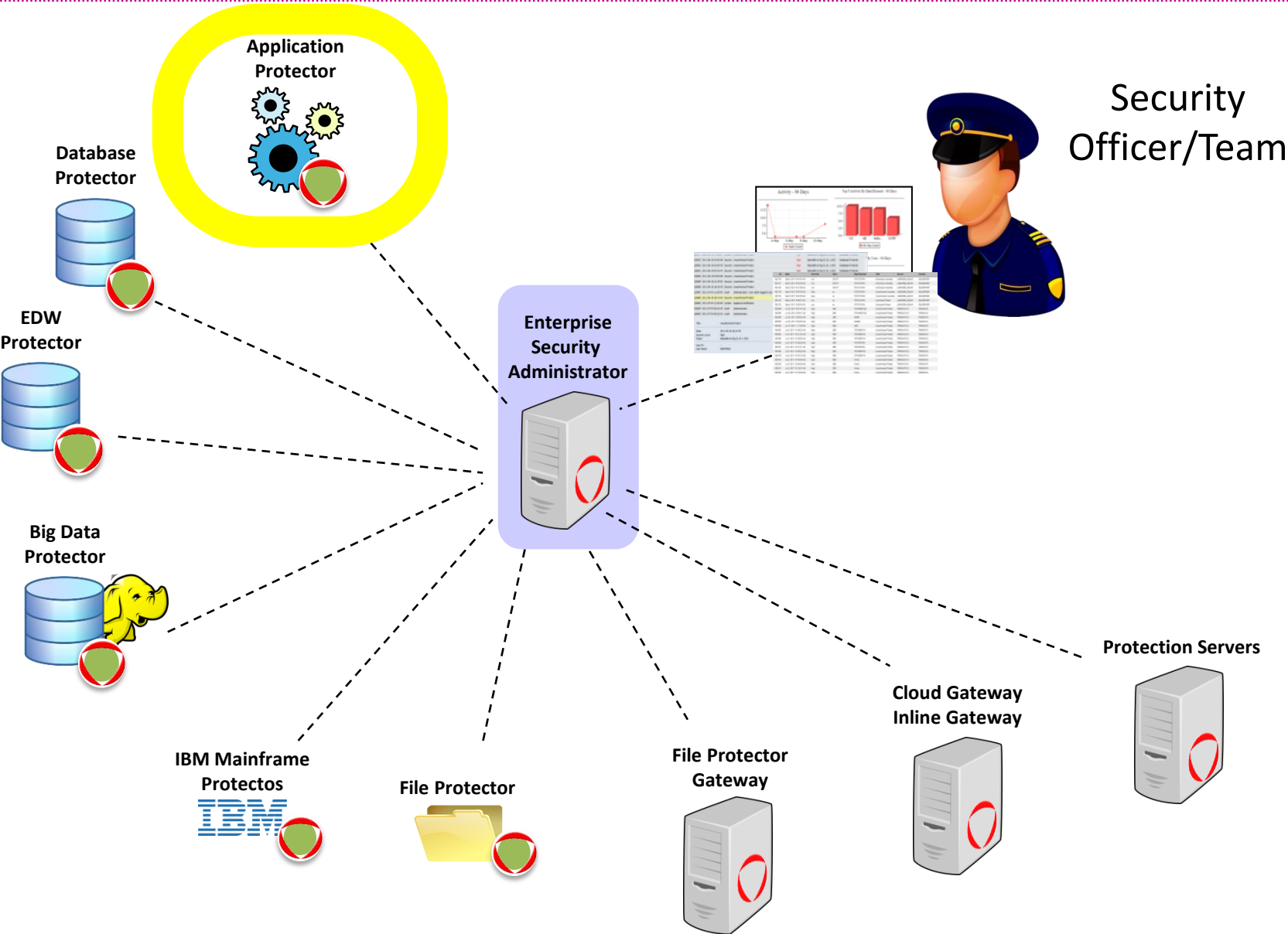
Vue d'ensemble de protegrity



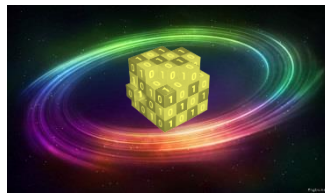
Où est le



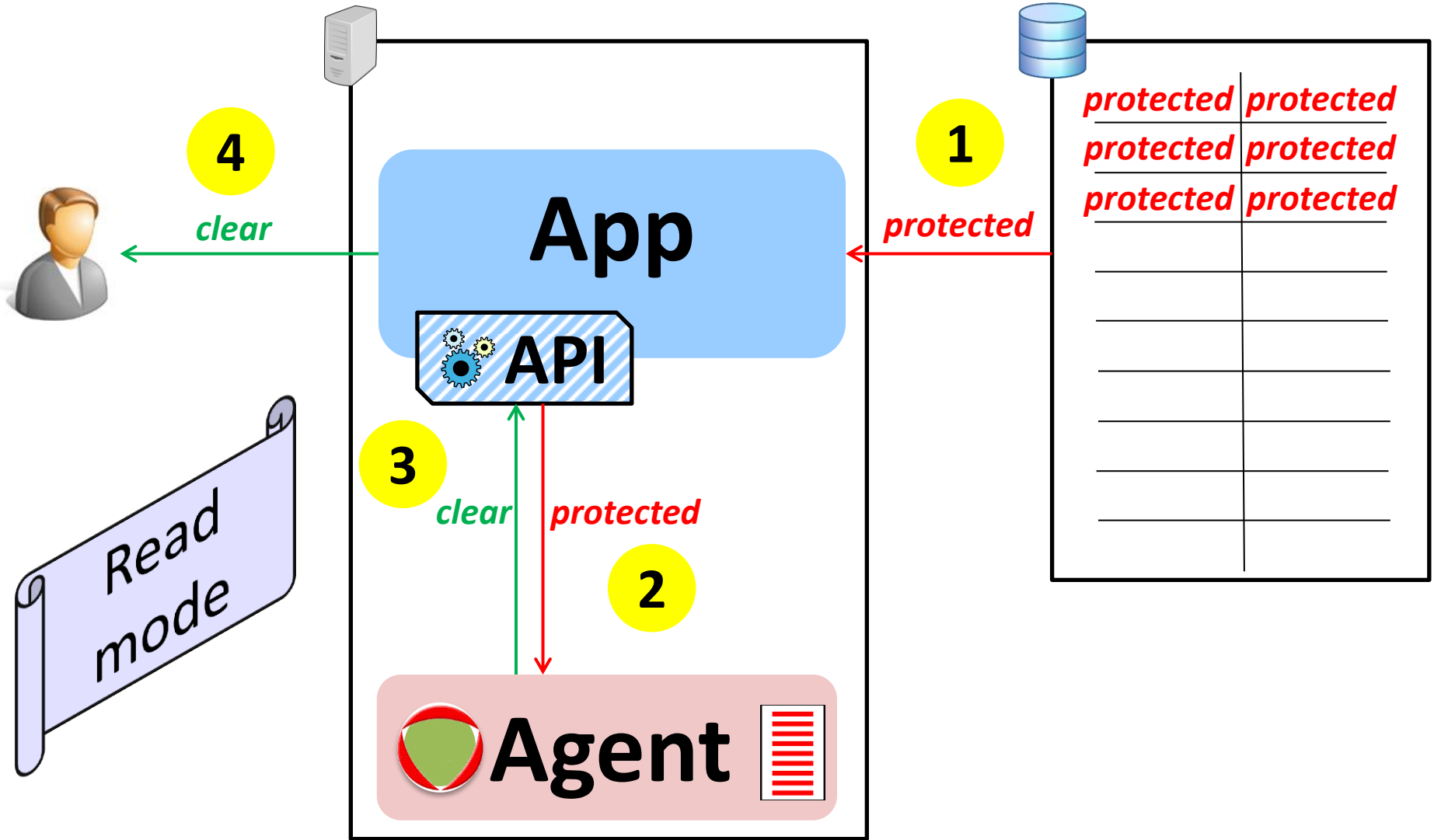
chez  protegrity ?



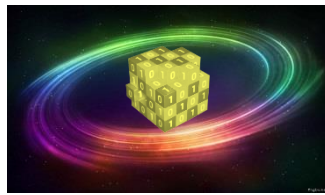
Le



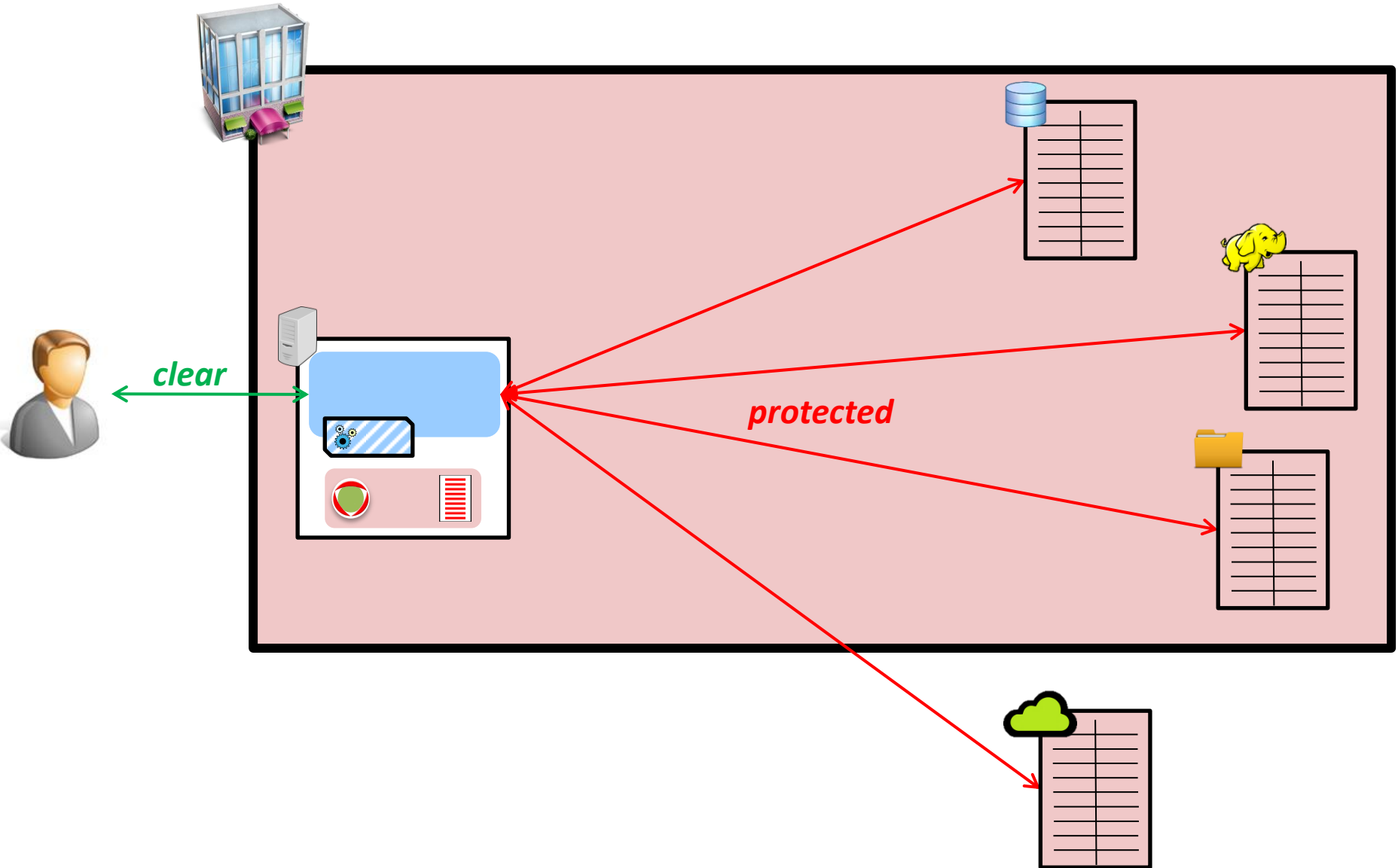
chez  protegrity



Le



chez  protegrity



Le



chez protegrity *en détail*

Unauthorized user

- DBA, sysadmin
- Developer, tester



Presentation to user

Name: cZu TusLPf

Address: 548 Xrk maYHq, 3549, Bruxelles-Capitale

Enterprise Security Administrator



Audit Logs



Agent



Not Authorized



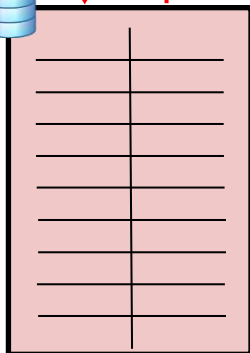
Allow to access the data?

Name: cZu TusLPf

Address: 548 Xrk maYHq, 3549, Bruxelles-Capitale

Name: cZu TusLPf

Address: 548 Xrk maYHq, 3549, Bruxelles-Capitale



at-rest

Name: cZu TusLPf

Address: 548 Xrk maYHq, 3549, Bruxelles-Capitale

Code pour faire



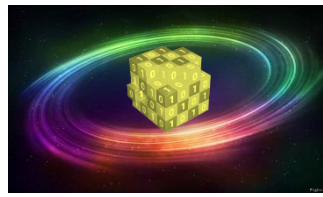
avec  protegrity

Il y a seulement
quelques adaptations
à faire dans les apps !

bien faites



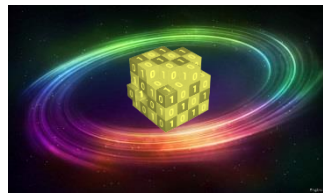
Code pour faire



avec  protegrity

```
public class Dummy {  
  
    /*  
        LOGIN FIRST  
    */  
    void login(Protegrity prot, String userName) {  
        prot.login(userName);  
    }  
  
    /*  
        LOGOUT AT THE END OF THE SESSION  
    */  
    void logout(Protegrity prot, String userName) {  
        prot.logout(userName);  
    }  
  
    .....  
  
}
```

Code pour faire



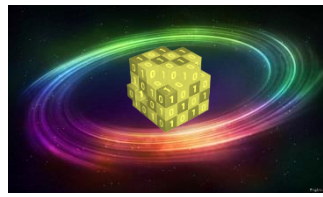
avec  protegrity

```
public class Dummy {
.....
/*
READ AND UNPROTECT DATA
*/
void readTable(Protegrity prot, Connection conn) {
    Statement stmt = conn.createStatement();

    //READ ORIGINAL TABLE
    ResultSet rs = stmt.executeQuery("SELECT * FROM NORTH_TABLE");
    ResultSetMetaData rsmd = rs.getMetaData();
    int columnsNumber = rsmd.getColumnCount();

    //FOR ALL THE PROTECTED RESULTS:
    while (rs.next()) {
        //UNPROTECT DATA
        String name = prot.unprotect("Name", rs.getString(0));
        Date date = prot.unprotect("Birthdate", rs.getDate(1));
    }
    rs.close();
    stmt.close();
}
.....
}
```

Code pour faire



avec  protegrity

```
public class Dummy {
.....

/*
PROTECT AND WRITE DATA TO DB
*/
void updateTable(Protegrity prot, Connection conn) {
    //PROTECT DATA
    String name = prot.protect("Name", "Jon Snow");
    String date = prot.protect("Birthdate", "20-02-1980");

    Statement stmt = conn.createStatement();

    //WRITE TO DB
    PreparedStatement prep = conn.prepareStatement("INSERT INTO NORTH_TABLE " +
        "(Name,Birthdate) VALUES (?,TO_DATE(?, 'DD-MM-YYYY'))");
    prep.setString(1, name);
    prep.setString(2, date);
    int result = prep.executeUpdate();
    stmt.close();
    prep.close();
}

.....

}
```





Recommendations

Points d'attentions pour



Méthode
légèrement
intrusive dans
les app

Effort minime de
re-engineering
pour mise en place

Travail lourd
de classification
des 

Batch toujours
possible via app

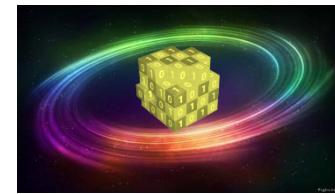
Fait 1 fois
pour toute

DBA toujours
capable de
faire son job

Accès direct
aux DB pas
compatible

Problématique avec
la *data quality*

Points d'attentions pour



Pas nécessaire
de protéger
toutes les



Protéger 1 système,
pas seulement 1



Prix élevé
du produit

Pas de partage
inter-institutionnel

Prix pour
formation
des employés

Complémentaire
aux protections
périphériques

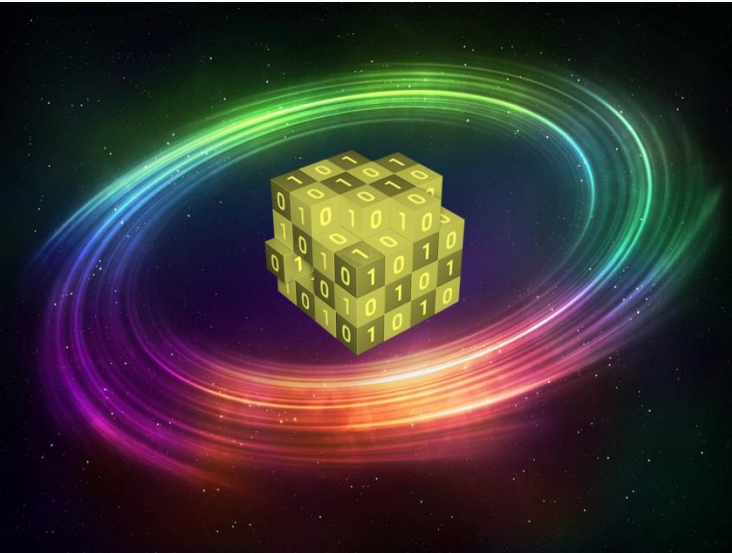
Augmente
la privacy

Conclusions

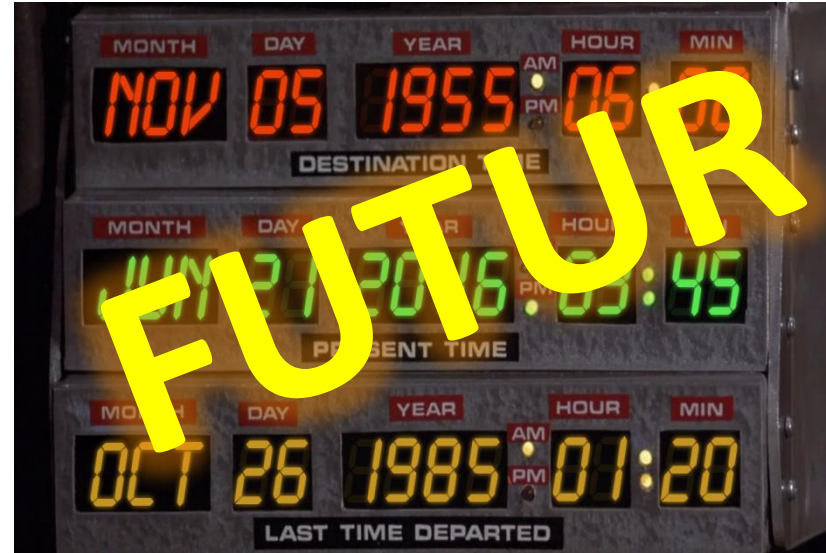


**= grande aide pour
être compatible avec la
General Data Protection Regulation**

Conclusions



=



Quelques intéressantes

- Tania Martin, "[Advanced Persistent Threats – Etat de l'Art](#)"
- Tania Martin, "[Social Engineering : watch out because there is no patch for human stupidity](#)"
- Information Is Beautiful, "[World's Biggest Data Breaches](#)"
- Bob Lannoy, "[Privileged Account Management \(PAM\)](#)"
- Johan Loeckx, "[Database Activity Monitoring \(DAM\)](#)"
- Kristof Verslype, "[Security Information and Event Management \(SIEM\)](#)"
- Delorean clock, <http://www.int33h.com/test/tc/>



Tania Martin

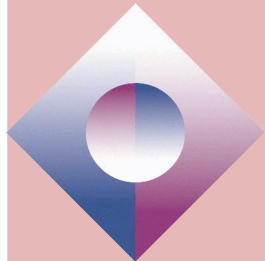


02 787 56 05



tania.martin@smals.be

Smals



www.smals.be



@Smals_ICT



www.smalsresearch.be



@SmalsResearch

