



Introduction à **CLOUD ENCRYPTION**

Comment protéger la confidentialité
des données hébergées dans le cloud

Julien Cathalo

Section Recherches

Agenda

1. Introduction
2. Applications de stockage dans le Cloud
3. Autres applications SaaS
4. Smals Threshold Encryption pour le Cloud
5. Recommandations

**Question et
remarques
bienvenues !**



Le Cloud

- Définition du NIST (National Institute of Standards and Technology) :

*« Cloud computing is a model for enabling ubiquitous, convenient, on-demand **network access** to a shared pool of configurable **computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”*



Le Cloud

- L'entreprise utilise des *ressources*



- Traditionnellement : l'entreprise *achète* et *entretient* ces ressources (comme des produits)
- Avec le Cloud Computing : l'entreprise *loue* ces ressources à un fournisseur (comme un service)

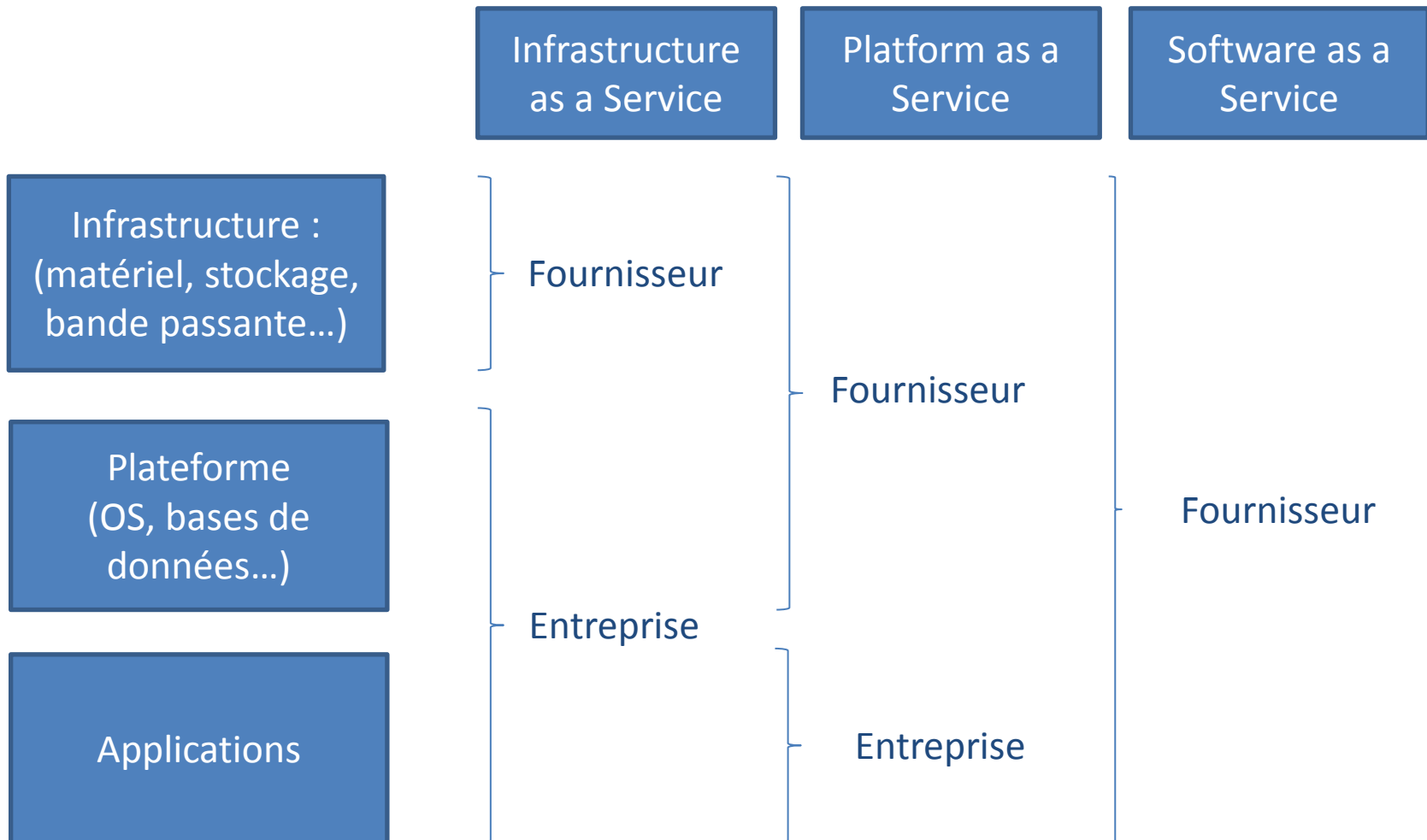


Avantages du Cloud

- Réduction des coûts
 - Licences
 - Coût d'entretien du matériel
 - Coût d'administration des logiciels
- Agilité
 - Ressources adaptées aux besoins
 - Ressources disponibles rapidement



Trois types de services Cloud



Sécurité dans le Cloud

- Sécurité :
 - Un des challenges du Cloud
 - Un frein à son adoption



During the cloud migration process, data protection security (72 percent) was cited as the top obstacle to a successful implementation of cloud services.

(2012 Cisco Global Cloud Networking Survey)



Sécurité dans le Cloud

Une peur parfois irrationnelle...

- Mesures de sécurité prises par les fournisseurs Cloud
- Dans certains cas passer au Cloud est un *gain* de sécurité !

... mais

- Aucun fournisseur n'est infaillible
- Ils sont parfois soumis à des lois (Patriot Act...)
- Gartner 2012 : ne faites pas confiance à votre fournisseur Cloud pour protéger vos données !

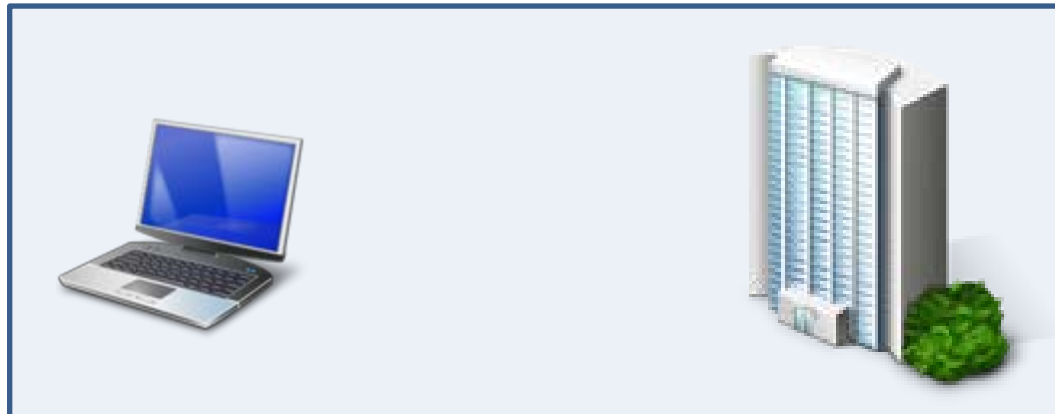


Confidentialité

- Security : « C.I.A. »
Confidentiality + Integrity + Availability
- Confidentialité
 - Empêcher l'accès non autorisé aux données
- Mise en œuvre :
 - Chiffrement des données (ex: AES 256 bits)
 - Mesures de gestion de clés



Confidentialité dans le Cloud



Protection des données

- Les données peuvent intéresser :
 - Un attaquant interne
 - Le fournisseur Cloud
 - Un attaquant externe
 - Un gouvernement



**Recommandation
n°1 : Les données
doivent être
chiffrées !**



Dropbox 2011

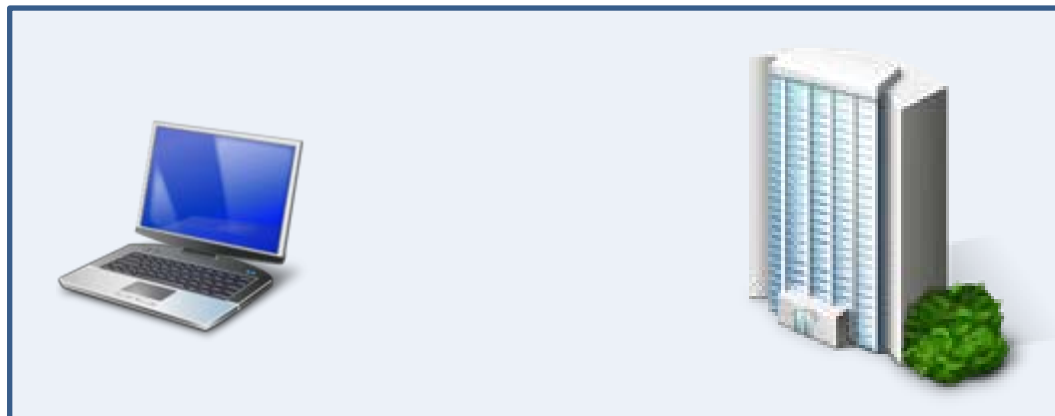
Dropbox Lied to Users About Data Security, Complaint to FTC Alleges

BY RYAN SINGEL  05.13.11 4:54 PM

- Avant le 13 avril 2011 :
“All files stored on Dropbox servers are encrypted (AES256) and are inaccessible without your account password.”
- Après le 13 avril 2011 :
“All files stored on Dropbox servers are encrypted (AES256).”



Dropbox 2011



Gestion des clés

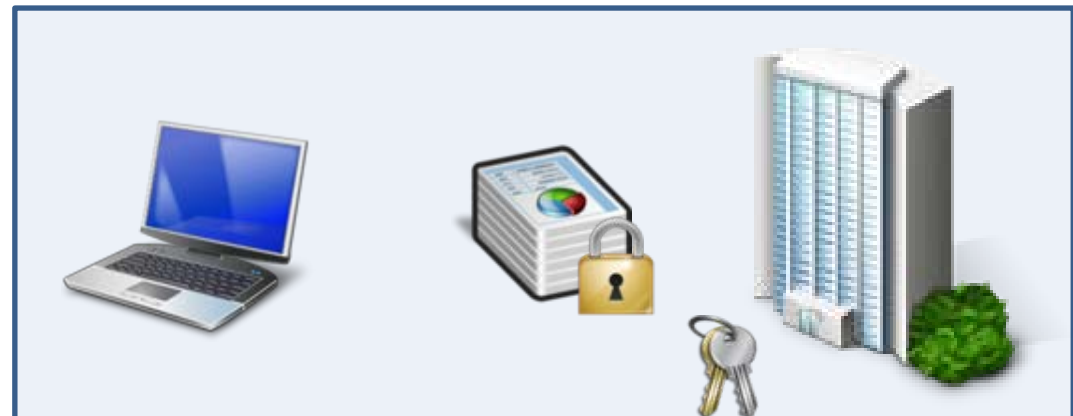
- Si c'est le fournisseur Cloud qui gère les clés
 - Le fournisseur peut accéder aux données
 - Le gouvernement peut accéder aux données
 - USA : Patriot Act
- Le fait que les données soient chiffrées n'est donc pas suffisant

Constat n°2 :
Les clés doivent être gérées par
l'utilisateur ou au sein de
l'entreprise !



Recommandation

- Chiffrer les données
- Garder le contrôle des clés
 - Les clés restent dans l'entreprise
- Indépendamment des mesures prises par le provider



Mise en oeuvre

- Utiliser des produits de Cloud Encryption adaptés à l'application
- Distinguer deux types d'applications :
 1. Les applications de stockage dans le Cloud (Box, Dropbox, Google Drive, SkyDrive...)
 2. Les autres applications SaaS (Google Apps, Office 365, Salesforce...)



Agenda

1. Introduction
2. Applications de stockage dans le Cloud
3. Autres applications SaaS
4. Smals Threshold Encryption pour le Cloud
5. Recommandations



Stockage dans le Cloud

- Répertoire local synchronisé automatiquement
- Quelques produits :



Stockage dans le Cloud

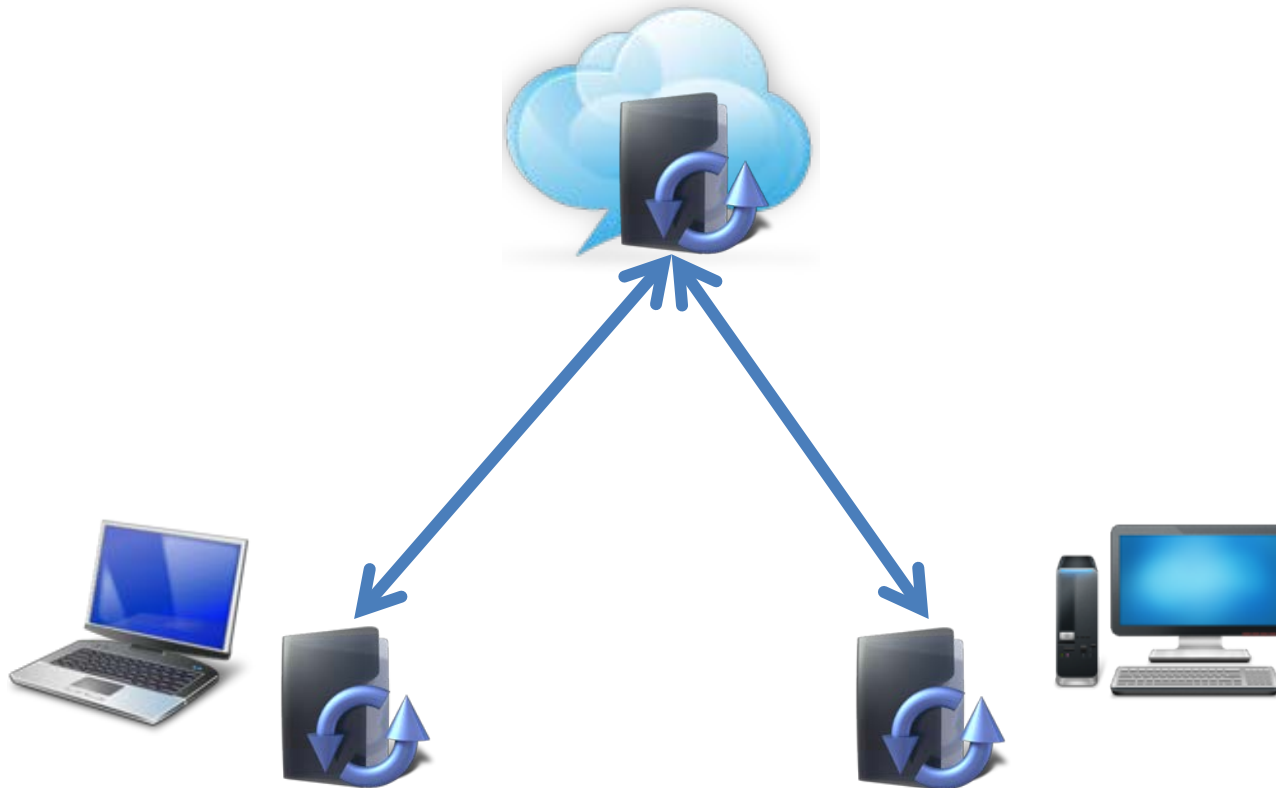
- Avantages :
 - Accéder aux mêmes données depuis plusieurs appareils



- Partager les données avec d'autres utilisateurs
- Réplication online (« backup »)



Stockage dans le cloud : Dropbox



Partage avec Dropbox

- Possibilité de partager un fichier ou répertoire avec d'autres personnes :
 - Non-utilisateurs de Dropbox
 - Lien vers un fichier
 - Envoi par mail
 - Permet la lecture du fichier
 - Utilisateurs de Dropbox
 - Partage d'un sous-répertoire du répertoire Dropbox
 - Apparaît dans le répertoire Dropbox de l'autre personne



Solutions de chiffrement

- Solutions dédiées pour utilisation avec service Cloud existant



- Solutions généralistes pour utilisation avec service Cloud existant



- Alternatives aux services existants



BoxCryptor



- Produit propriétaire payant avec version gratuite
- Solution de chiffrement pour répertoire local
- Possibilité de synchroniser ce répertoire avec un service cloud
- Chiffrement AES 256 bits
- Existe pour
 - Windows
 - Mac OS X
 - Android
 - iOS



BoxCryptor : Versions

PRICING

it's free!

	Free	Unlimited Personal	Unlimited Business
Price (one-time-fee)	Free	€ 29.99 / US\$ 39.99	€ 69.99 / US\$ 99.99
Number of Drives	1	Unlimited	Unlimited
Number of Devices & Encryption Volume	Unlimited	Unlimited	Unlimited
Number of Users	1	1	1
AES-256 Encryption	✓	✓	✓
Multi-Platform	✓	✓	✓
Free Apps for Android, iPhone and iPad	✓	✓	✓
Community Support	✓	✓	✓
Filename Encryption		✓	✓
Commercial Usage			✓

User License ▾

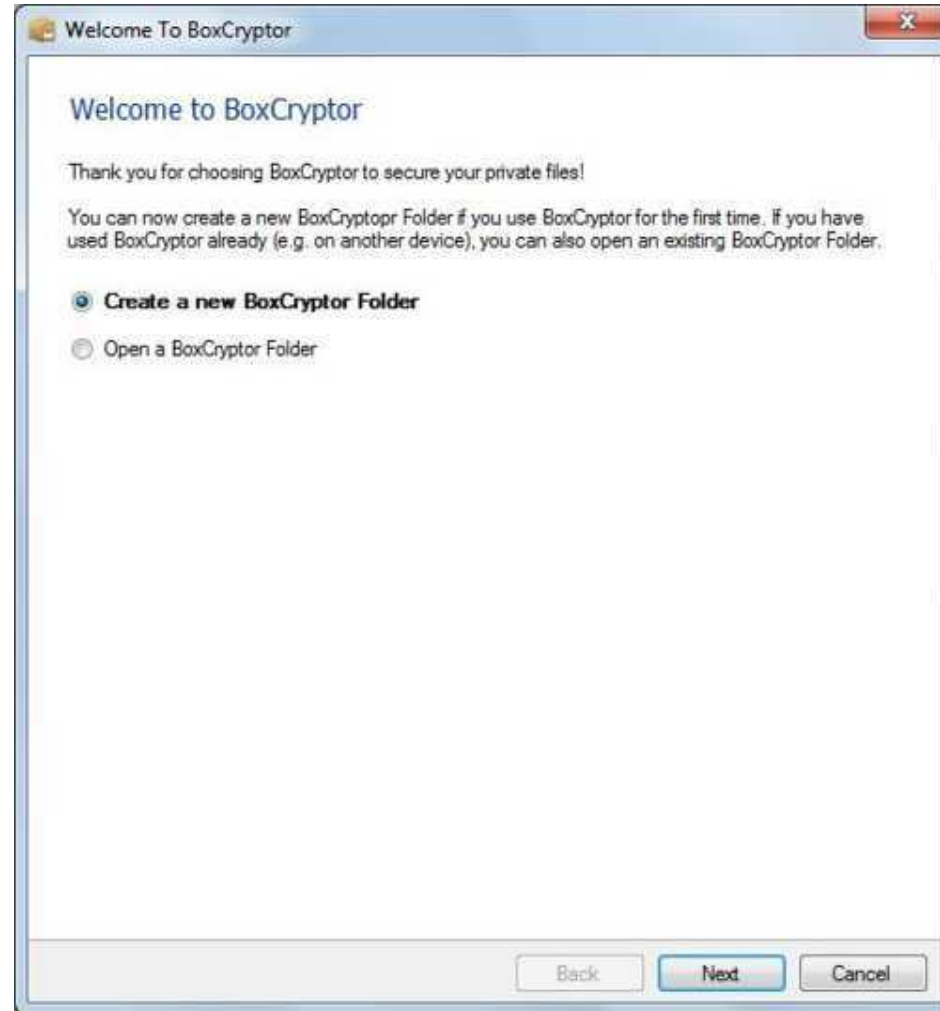
User License ▾

Buy now

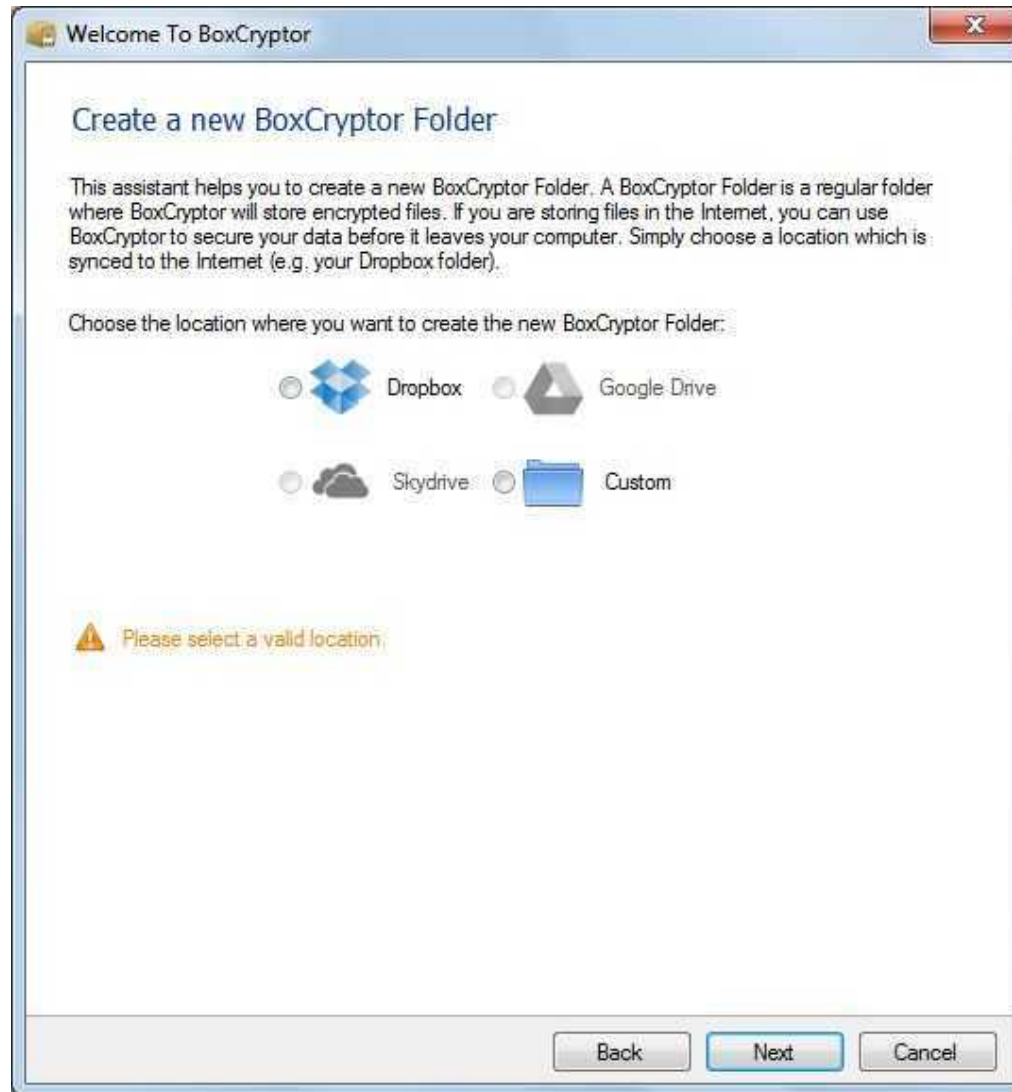
Buy now



BoxCryptor : Configuration



BoxCryptor : Configuration



BoxCryptor : Disque Virtuel



BoxCryptor : Choix du mot de passe



Welcome To BoxCryptor

Create a password

BoxCryptor secures the encrypted files with the password entered here. It is recommended to use a secure password with at least 6 characters including numbers and symbols.

IMPORTANT: It is absolutely not possible to restore or reset your password in case you do not remember it anymore! If you forget this password, the data of your encrypted files will be lost!

Please make sure not to forget this password! We recommend to write it down on paper and store it in a secure place (e.g. in a safe).

New Password:

Confirm Password:

Show Password

Remember this password

Back Finish Cancel

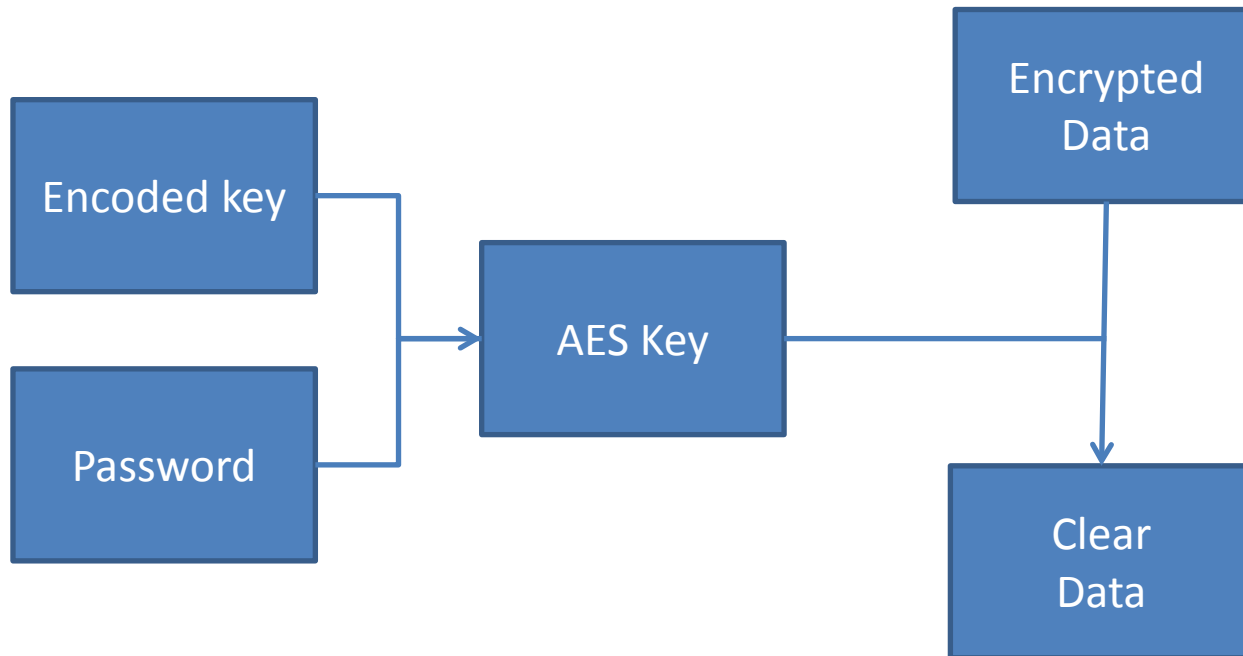


BoxCryptor : Backup du fichier de configuration



Chiffrement BoxCryptor

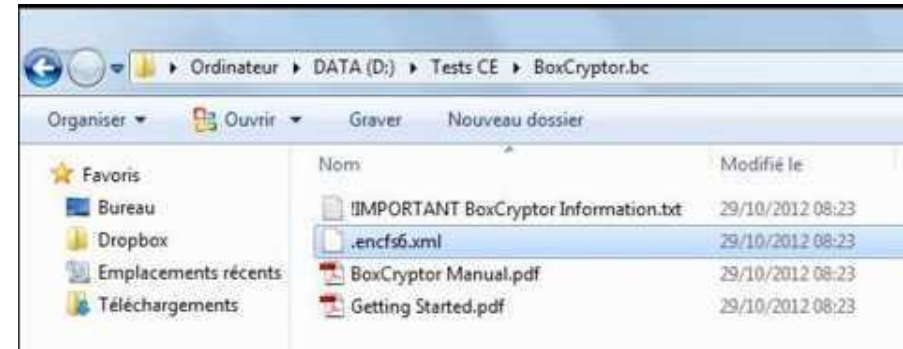
- BoxCryptor a généré une clé AES 256 bits à l'installation
- Elle est utilisée pour chiffrer / déchiffrer les données
- Elle est stockée (« encoded key ») sous forme protégée par mot de passe dans le fichier de configuration



Répertoire et disque virtuel

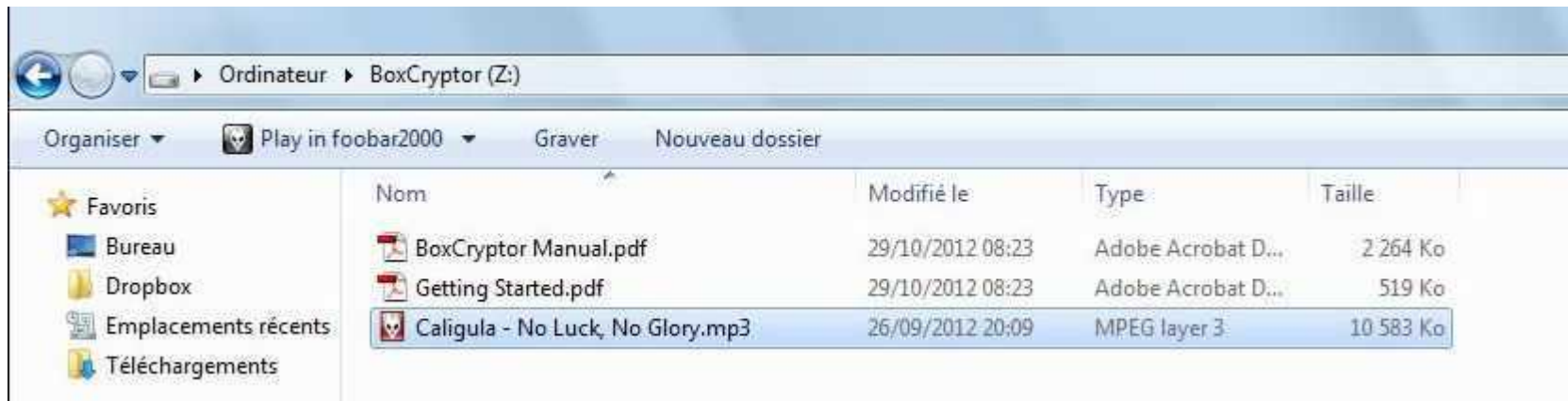
- Répertoire BoxCryptor :
 - Situé sur mon disque dur
 - Contient mon fichier de configuration
 - Contient mes fichiers chiffrés
 - Est synchronisé avec Dropbox ou autre

- Disque virtuel
 - Porte la lettre Z:
 - Me présente mes fichiers en clair



Copions un mp3 dans Z:

- BoxCryptor le chiffre à la volée.



Lecture du mp3

The screenshot shows a Windows XP desktop environment. In the background, a Windows Explorer window is open to the 'BoxCryptor (Z:)' drive. The file list contains:

Nom	Modifié le	Type	Taille
BoxCryptor Manual.pdf	29/10/2012 08:23	Adobe Acrobat D...	2.264 Ko
Getting Started.pdf	29/10/2012 08:23	Adobe Acrobat D...	519 Ko
Caligula - No Luck, No Glory.mp3	26/09/2012 20:09	MPEG layer 3	10.583 Ko

In the foreground, a music player window titled 'Caligula - [2012 SAE] No Luck, No Glory. [foobar2000 v1.1]' is open. The 'Properties' tab is selected, showing the following metadata:

Name	Value
Metadata	
Artist Name	Caligula
Track Title	No Luck, No Glory
Album Title	2012 SAE
Date	2012
Comment	00001735 00001150 0000B56C 00008

The 'Playlists' tab is also visible, showing a playlist named 'New Playlist' with one track:

Title / track artist	Duration	Item index
Caligula - [2012] 2012 SAE No Luck, No Glory	4:31	1

A pink box with the text 'La lecture fonctionne.' is overlaid on the music player window. At the bottom of the music player window, the status bar shows: 'MP3 | 320 kbps | 44100 Hz | stereo | 1:11 / 4:31'. An equalizer is also visible at the bottom of the window.



Lecture du mp3 chiffré

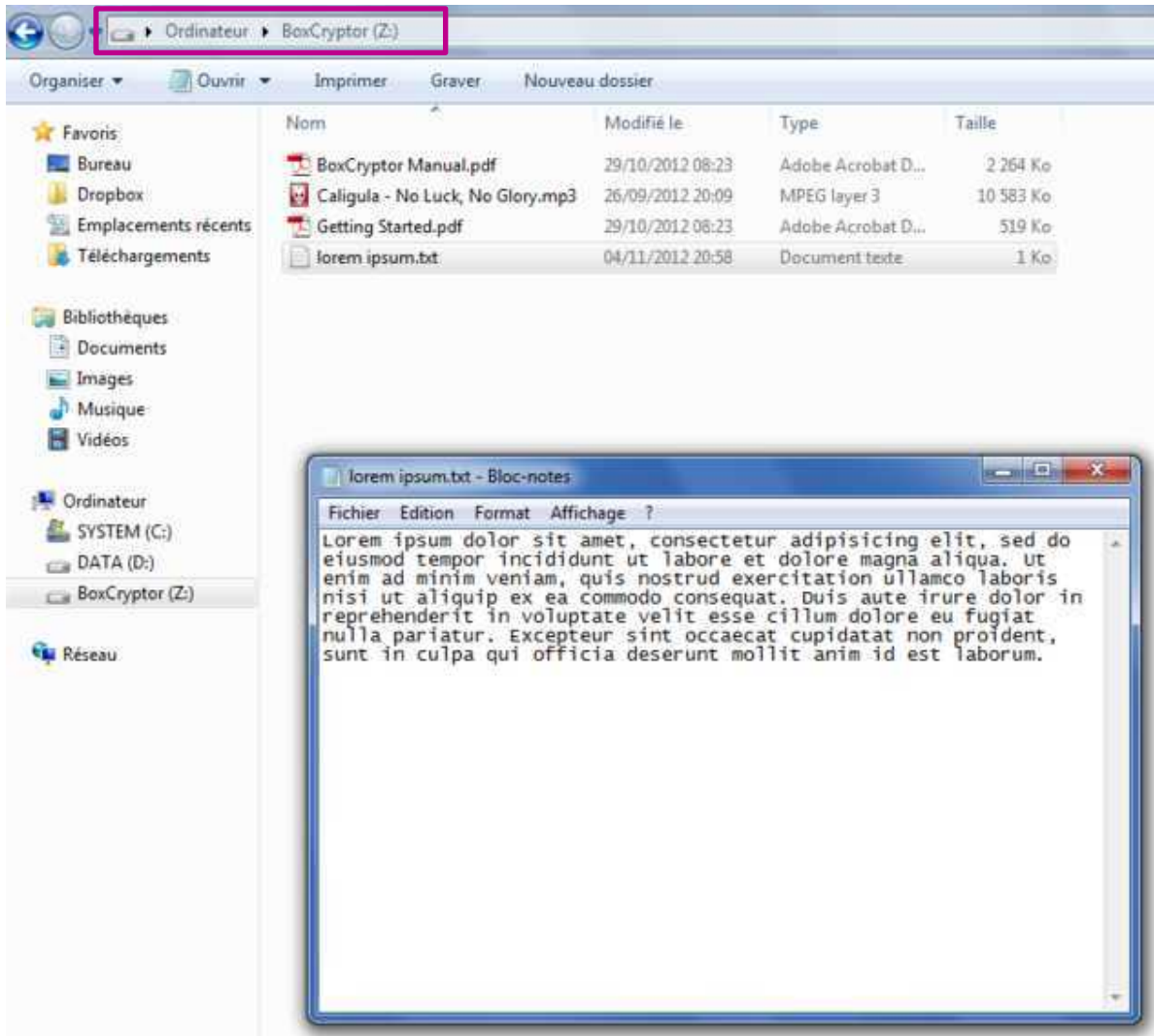
The screenshot shows a Windows Explorer window with the address bar set to 'Ordinateur > DATA (D:) > Tests CE > BoxCryptor.bc'. The file list contains:

Nom	Modifié le	Type	Taille
!IMPORTANT BoxCryptor Information.txt	29/10/2012 08:23	Document texte	1 Ko
.encfs6.xml	29/10/2012 08:23	Document XML	2 Ko
BoxCryptor Manual.pdf	29/10/2012 08:23	Adobe Acrobat D...	2 264 Ko
Caligula - No Luck, No Glory.mp3	26/09/2012 20:09	MPEG layer 3	10 583 Ko
Getting Started.pdf	29/10/2012 08:23	Adobe Acrobat D...	519 Ko

The foobar2000 v1.1 window is open, showing a playlist with the text 'Fichier illisible.' (File unreadable) overlaid on the track list area. The status bar at the bottom of the player indicates 'Stopped'.



Fichier texte en clair



The screenshot shows a Windows Explorer window with the address bar set to 'Ordinateur > BoxCryptor (Z:)'. The file list contains:

Nom	Modifié le	Type	Taille
BoxCryptor Manual.pdf	29/10/2012 08:23	Adobe Acrobat D...	2 264 Ko
Caligula - No Luck, No Glory.mp3	26/09/2012 20:09	MPEG layer 3	10 583 Ko
Getting Started.pdf	29/10/2012 08:23	Adobe Acrobat D...	519 Ko
loreem ipsum.txt	04/11/2012 20:58	Document texte	1 Ko

The 'loreem ipsum.txt' file is selected, and a Notepad window titled 'loreem ipsum.txt - Bloc-notes' is open, displaying the following text:

```
Fichier Edition Format Affichage ?
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore et dolore magna aliqua. ut
enim ad minim veniam, quis nostrud exercitation ullamco laboris
nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in
reprehenderit in voluptate velit esse cillum dolore eu fugiat
nulla pariatur. Excepteur sint occaecat cupidatat non proident,
sunt in culpa qui officia deserunt mollit anim id est laborum.
```



Fichier texte chiffré

The screenshot shows a Windows Explorer window with the address bar set to 'Ordinateur > DATA (D:) > Tests CE > BoxCryptor.bc'. The file list contains the following items:

Nom	Modifié le	Type	Taille
IMPORTANT BoxCryptor Information.txt	29/10/2012 08:23	Document texte	1 Ko
.encfs6.xml	29/10/2012 08:23	Document XML	2 Ko
BoxCryptor Manual.pdf	29/10/2012 08:23	Adobe Acrobat D...	2 264 Ko
Caligula - No Luck, No Glory.mp3	26/09/2012 20:09	MPEG layer 3	10 583 Ko
Getting Started.pdf	29/10/2012 08:23	Adobe Acrobat D...	519 Ko
lorem ipsum.txt	04/11/2012 20:58	Document texte	1 Ko

The 'lorem ipsum.txt' file is highlighted, and a Notepad window titled 'lorem ipsum.txt - Bloc-notes' is open over it. The text in the Notepad window is completely garbled, representing encrypted data.



Tests avec d'autres fichiers

- Test avec fichier vidéo, 200 Mo
 - Dans Z:, copie et lecture immédiates
 - Dans D:, fichier illisible
- Test avec répertoire de 10 Go
 - Copie depuis C: vers Z: 10 minutes
 - C'est le chiffrement ? NON !
 - Copie : 15 Mo/sec
 - Chiffrement : 50 Mo/sec (AES)
 - ***Dans ce test, le chiffrement n'a pas impacté les performances***



TrueCrypt

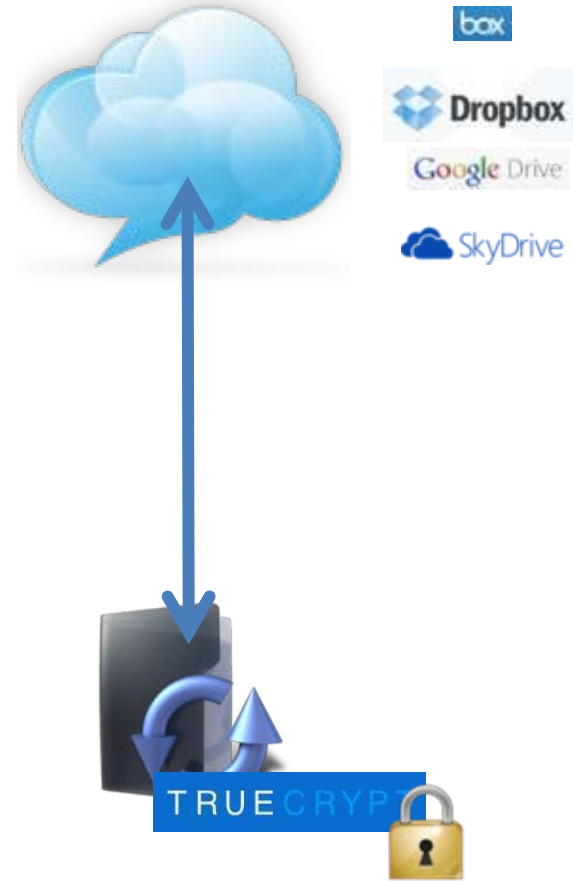


- Logiciel open-source
- Crée un répertoire virtuel chiffré
- Chiffrement à la volée
- Support d'algorithmes cryptographie standard
- Autres fonctionnalités plus avancées
- Existe pour
 - Windows
 - Mac OS X
 - Linux

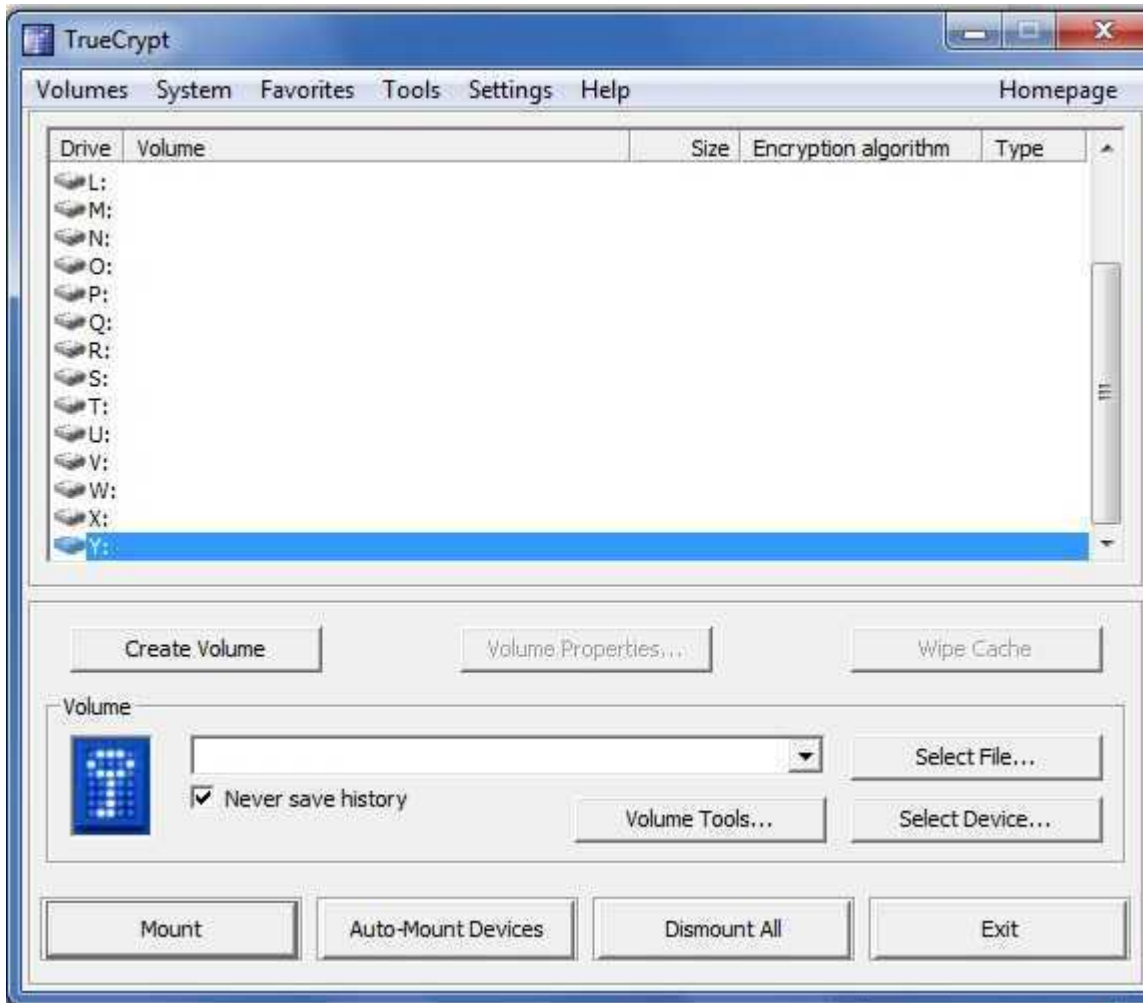


TrueCrypt

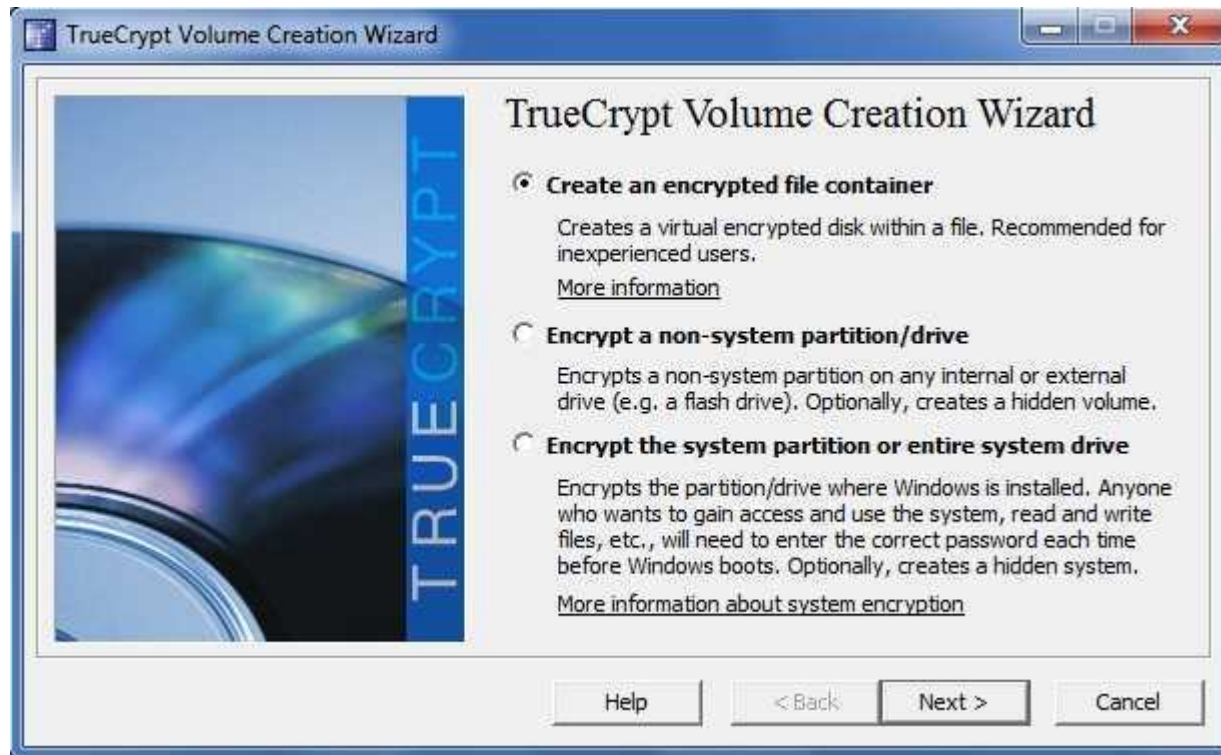
- Pas conçu pour être utilisé avec un service cloud
- Mais fonctionne parfaitement
- Peut-être utilisé comme BoxCryptor



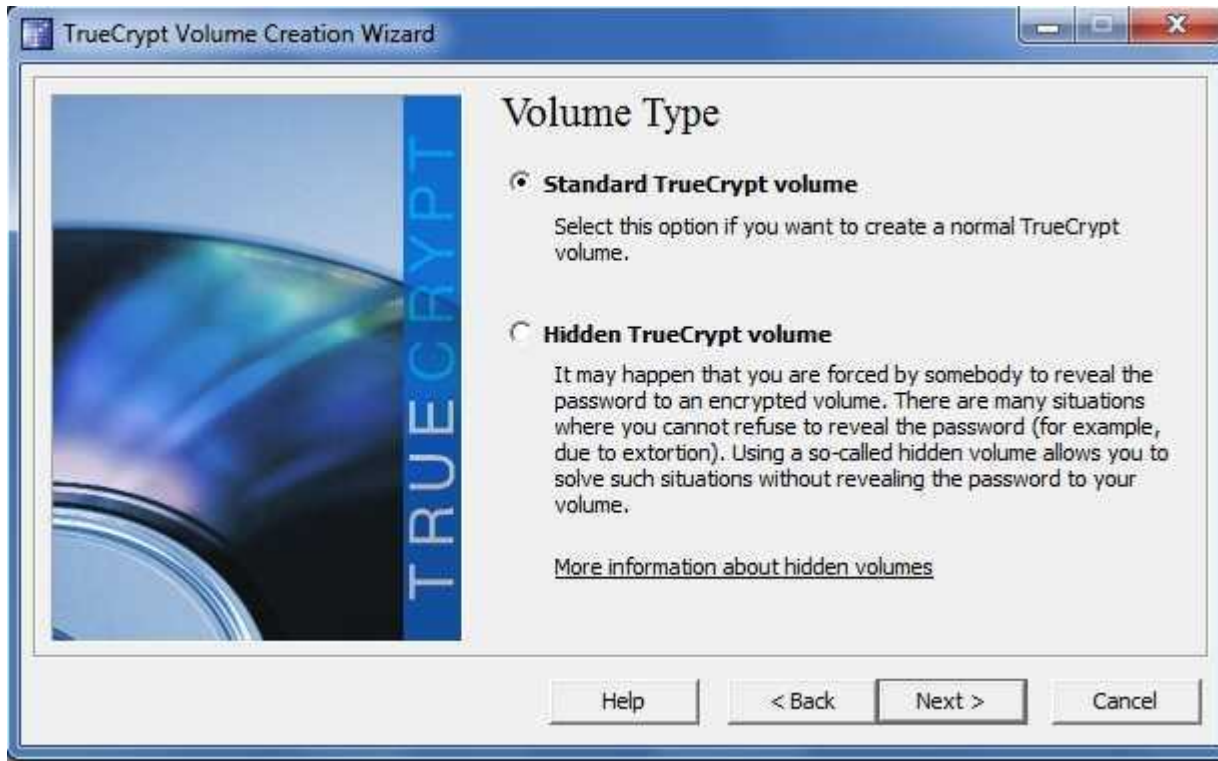
TrueCrypt : Choix du volume



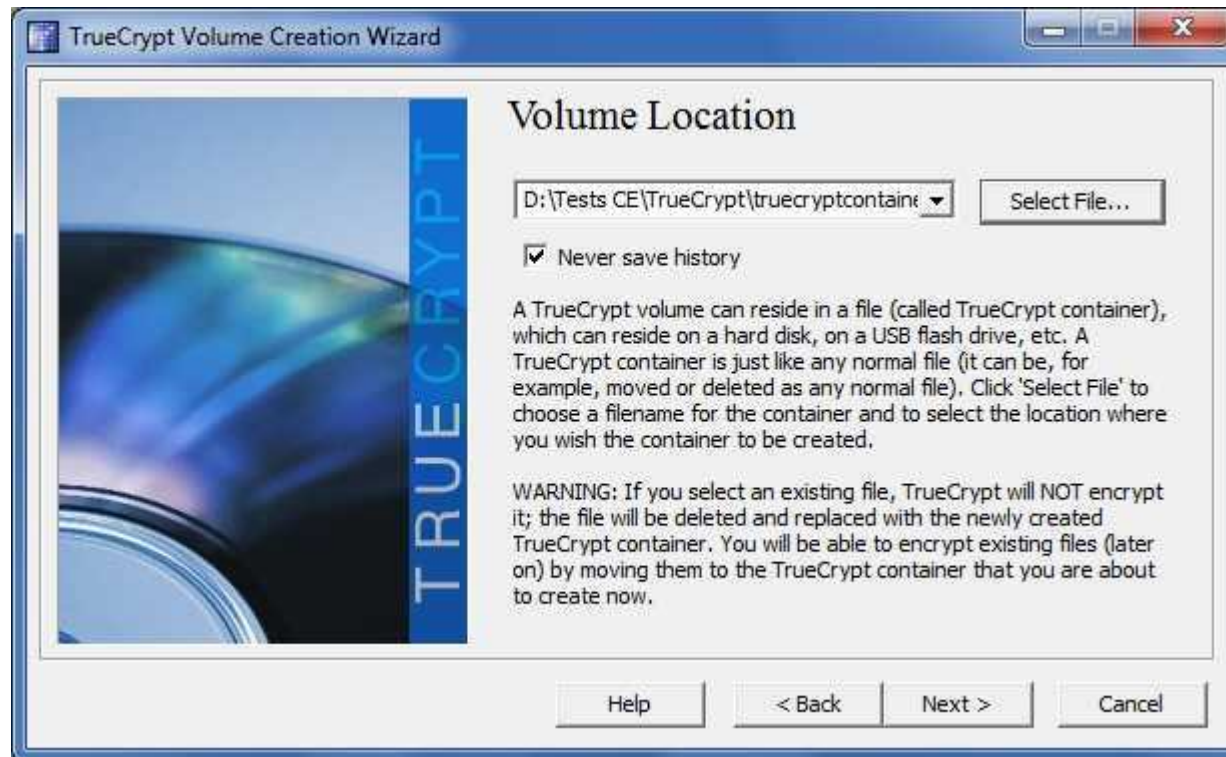
TrueCrypt : Container



TrueCrypt : Volume standard ou caché



TrueCrypt : Emplacement du container



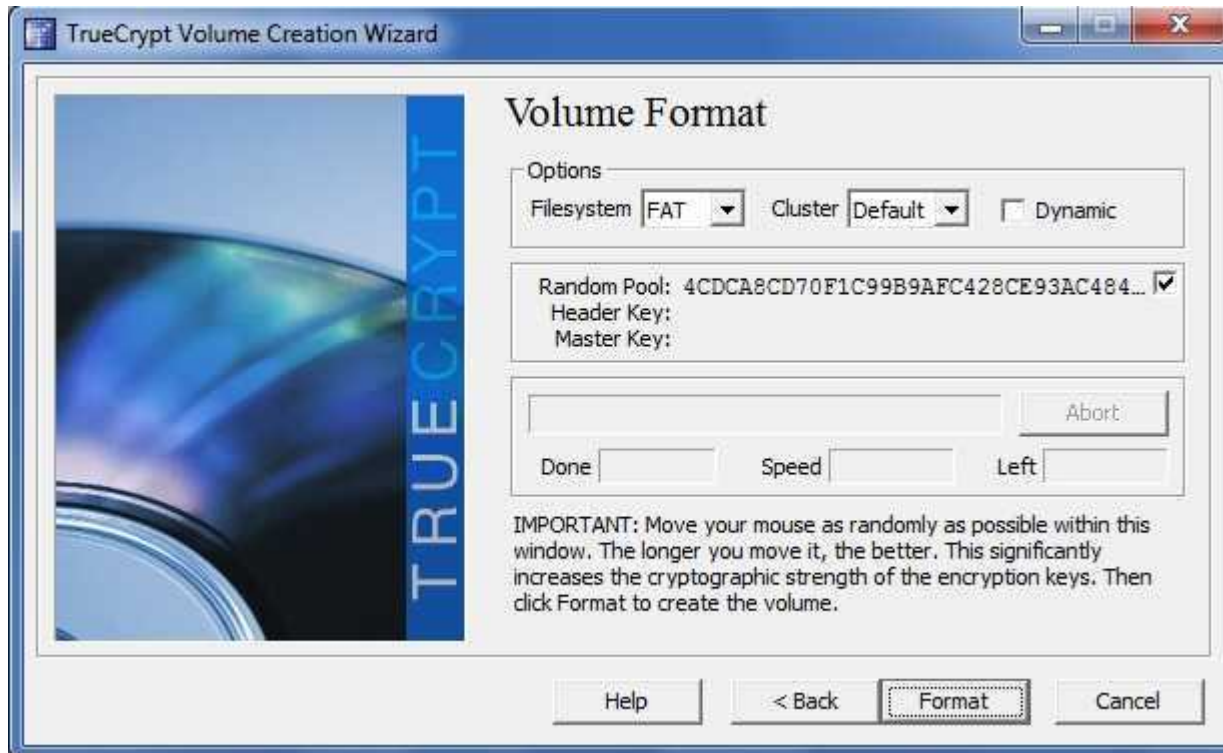
TrueCrypt : Options de chiffrement



TrueCrypt : Mot de passe



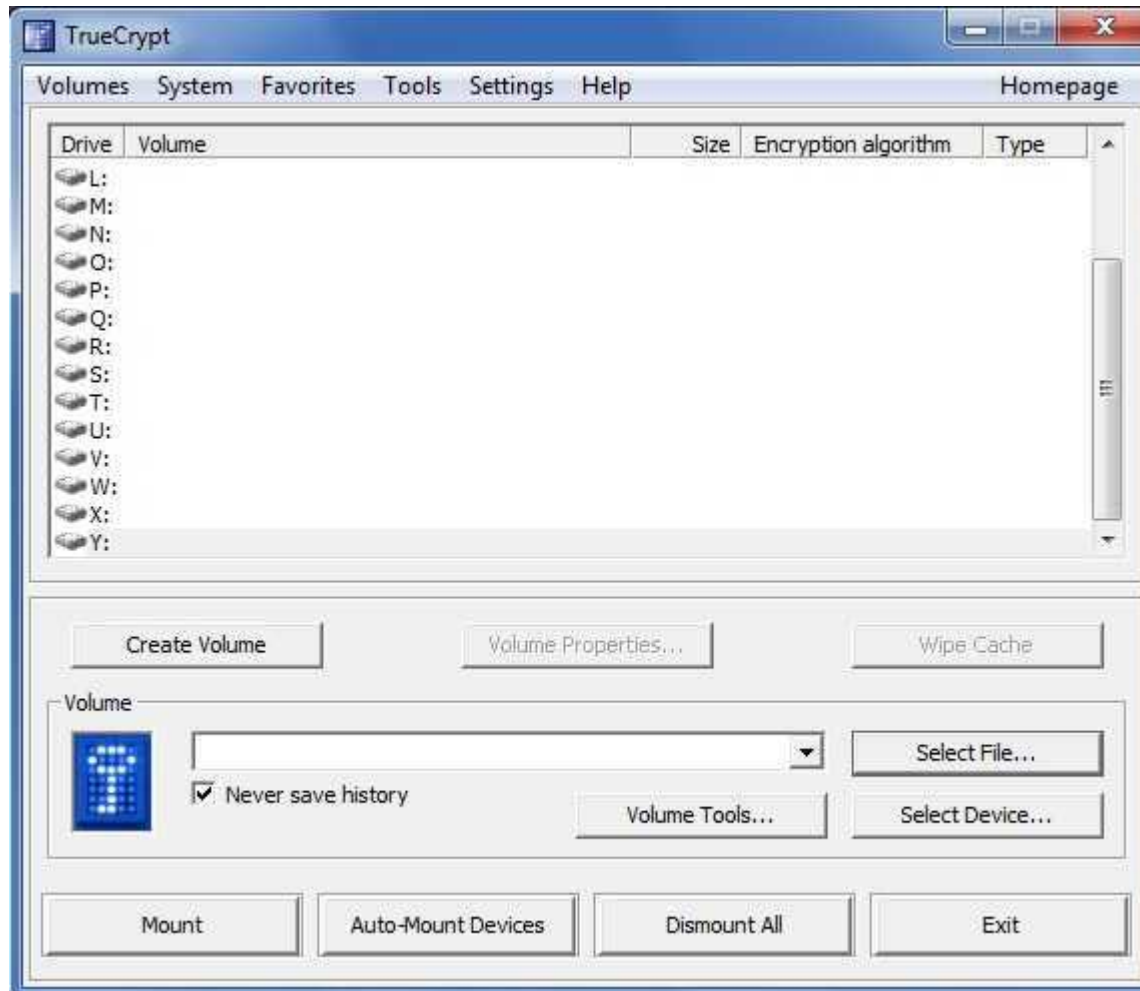
TrueCrypt : Génération de la clé



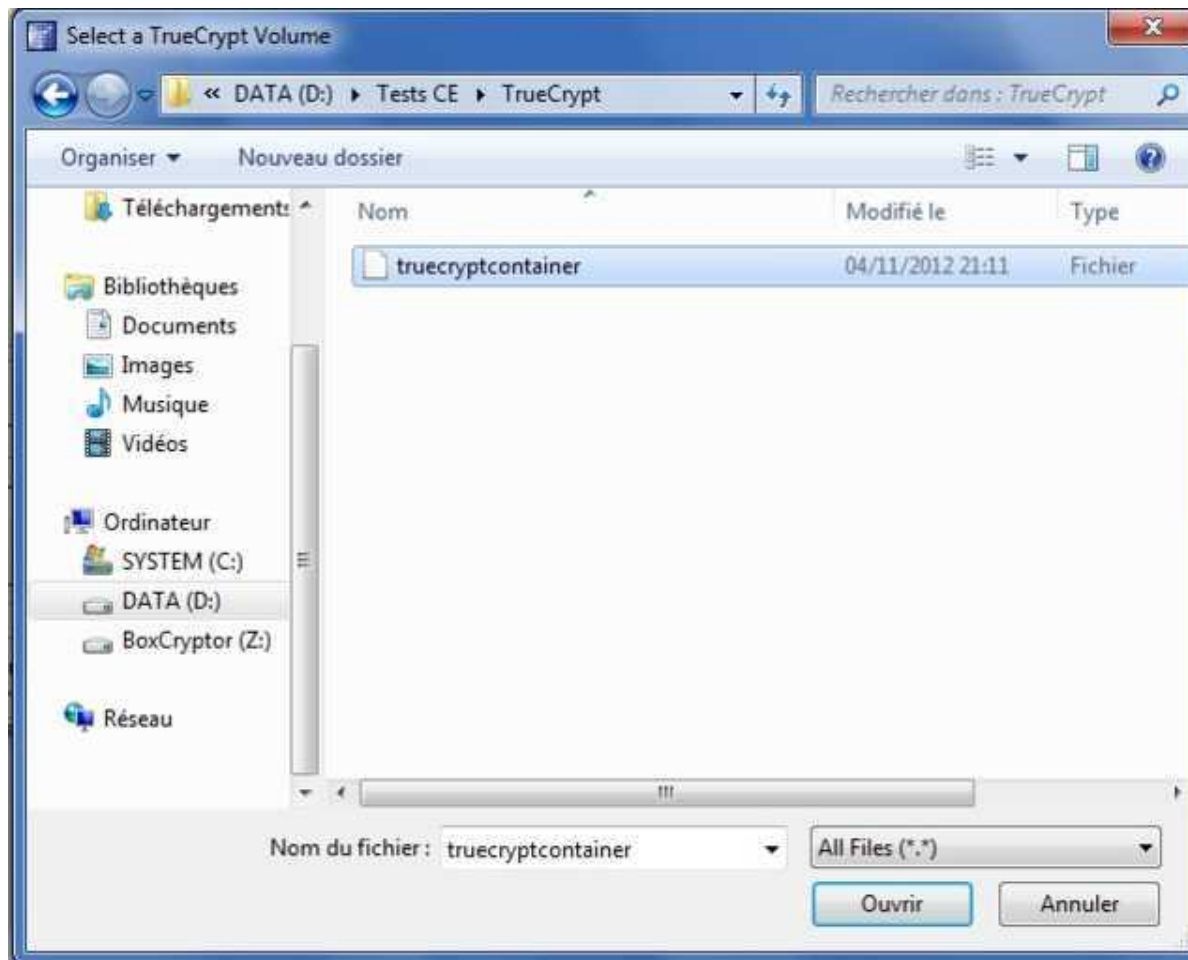
TrueCrypt : Finalisation



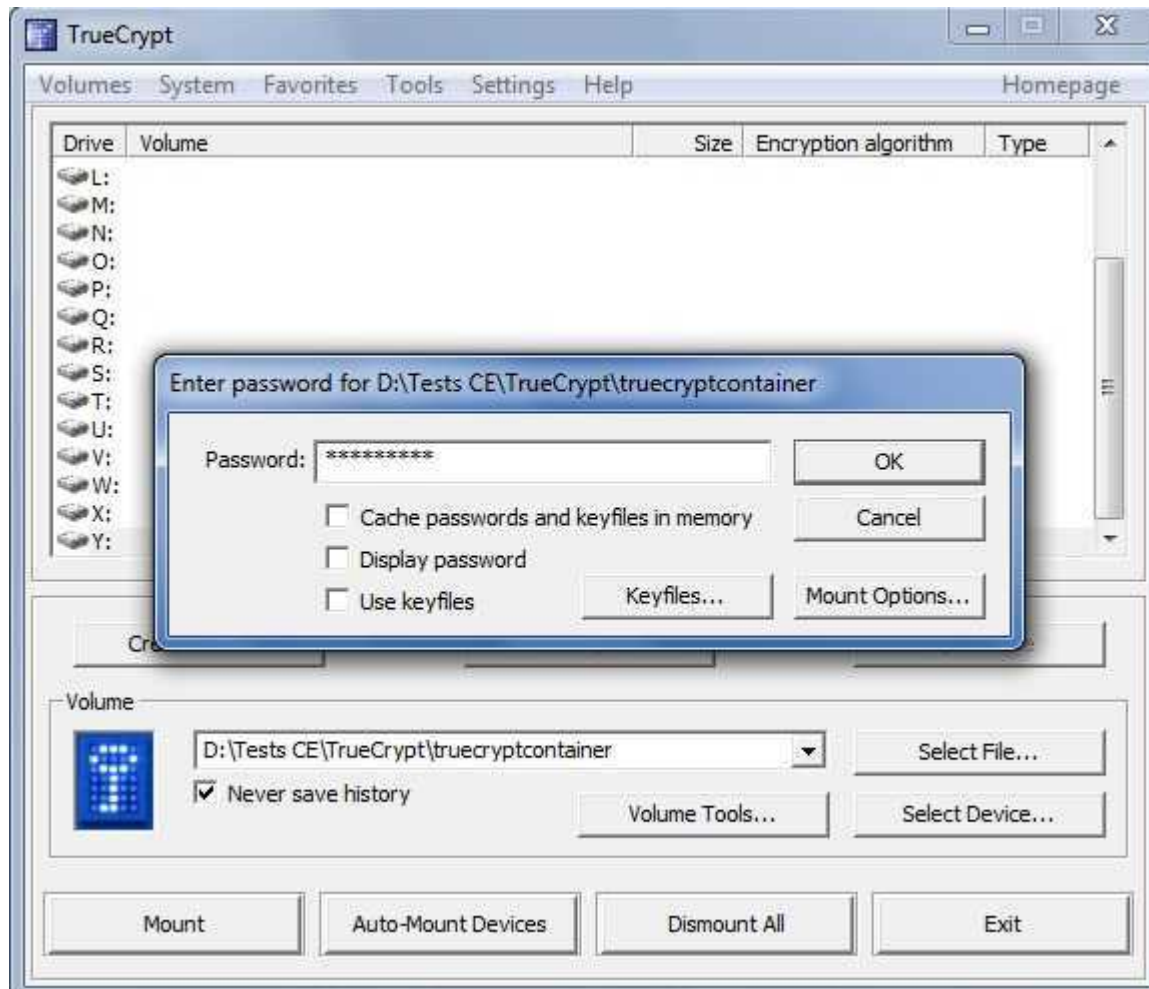
TrueCrypt : Montage du volume



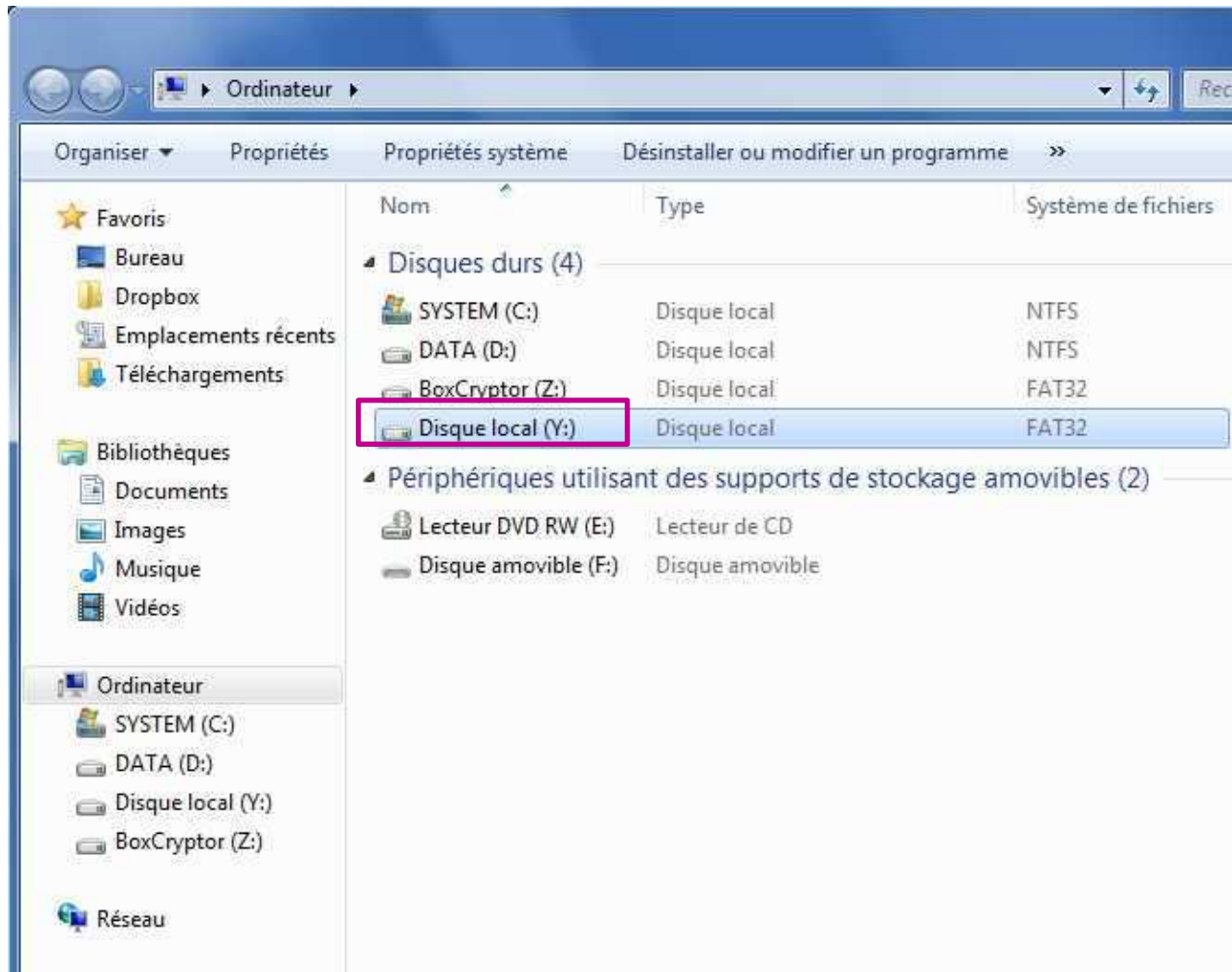
TrueCrypt : Emplacement du container



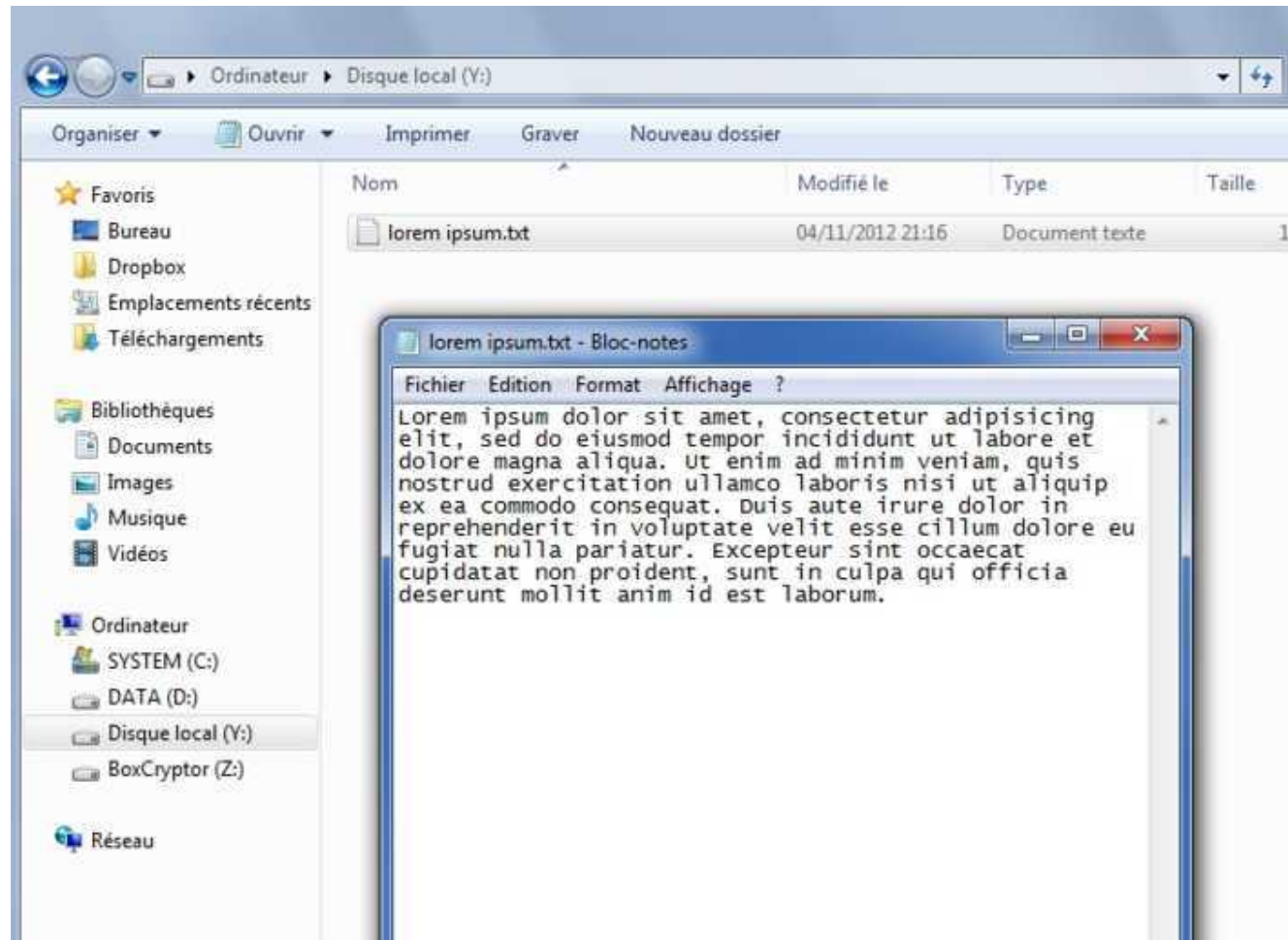
TrueCrypt : Entrée du mot de passe



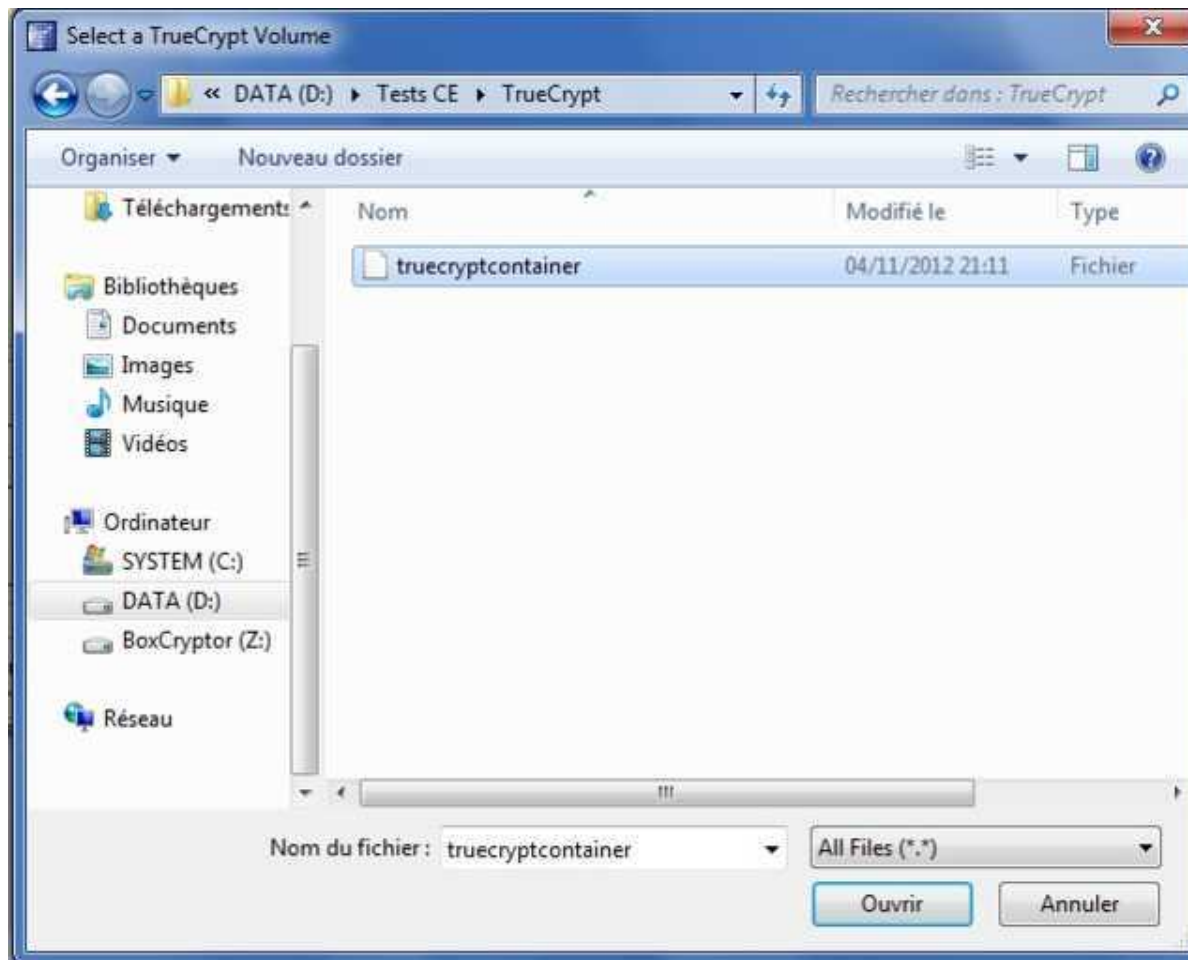
TrueCrypt : Disque virtuel



TrueCrypt : Fichier texte en clair



TrueCrypt : Fichier texte chiffré




TeamDrive

- Produit propriétaire payant avec version gratuite
- Offre simultanément
 - Service de stockage Cloud
 - Chiffrement
- Existe pour
 - Windows
 - Mac OS X
 - Linux
 - Android
 - iOS



Opinion du cryptologue

- Ces solutions se valent en termes de
 - ✓ – Choix de l'algorithme (Advanced Encryption Standard)
 - ✓ – Taille de clés (256 bits)
- Les différences sont :
 - La gestion des clés
 - L'implémentation
 - BoxCryptor : ???
 - ✓ • TrueCrypt : open-source, validé par la communauté
 - TeamDrive : validation par experts allemands 



Conclusion

- Pour accéder à ses données depuis plusieurs appareils :
 - Pas d'impact
- Pour partager des données avec d'autres utilisateurs :
 - Une seule option : partage du répertoire complet et du mot de passe
 - Perte de fonctionnalité
 - Inconvénient pratique
- Réplication online (« backup »)
 - Pas d'impact



Conclusion

- Ces produits permettent :
 - Utilisation transparente
 - Peu d'impact sur les performances
 - Certaines fonctionnalités préservées
 - Gain réel de sécurité
- Leurs limites :
 - Partage
 - Sécurité :
 - le fournisseur Cloud peut surveiller votre activité
 - le fournisseur Cloud peut connaître la taille des fichiers



Recommandation

- De préférence :
 - Utiliser TrueCrypt + service stockage Cloud
- Motivation :
 - TrueCrypt : meilleures garanties de sécurité
 - Mise en œuvre simple
 - Permet de séparer
 - le service de chiffrement
 - le service de stockage



Agenda

1. Introduction
2. Applications de stockage dans le Cloud
3. **Autres applications SaaS**
4. Smals Threshold Encryption pour le Cloud
5. Recommandations



Cloud Security Gateways : But

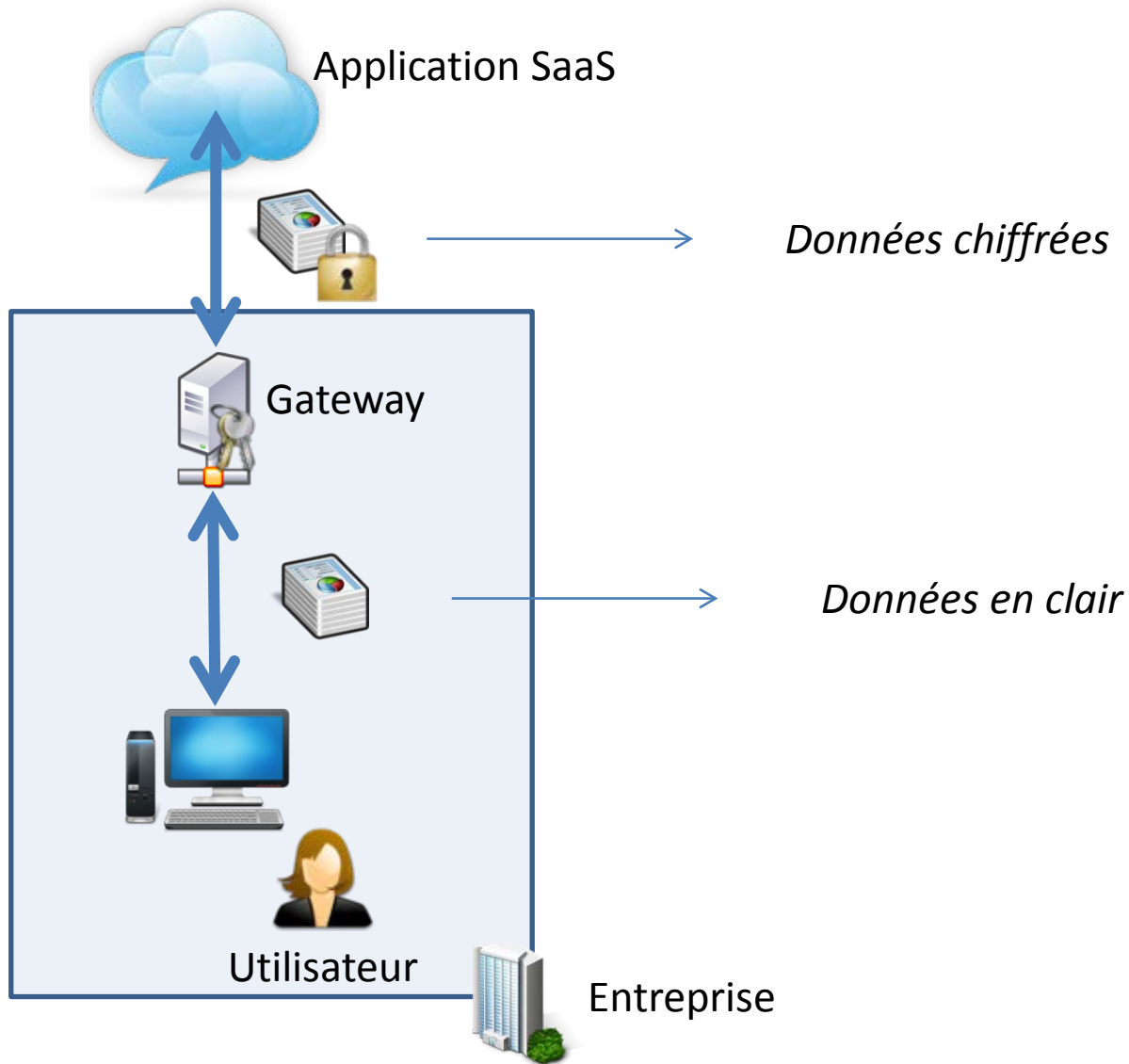
Permettre l'utilisation d'applications Software as a Service



en protégeant la confidentialité des données



Fonctionnement



Fonctionnement

- Le Cloud Security Gateway

- Connaît l'application SaaS

- Connaît la structure des données échangées

- Chiffre / déchiffre à la volée certains champs

- Laisse d'autres champs en clair

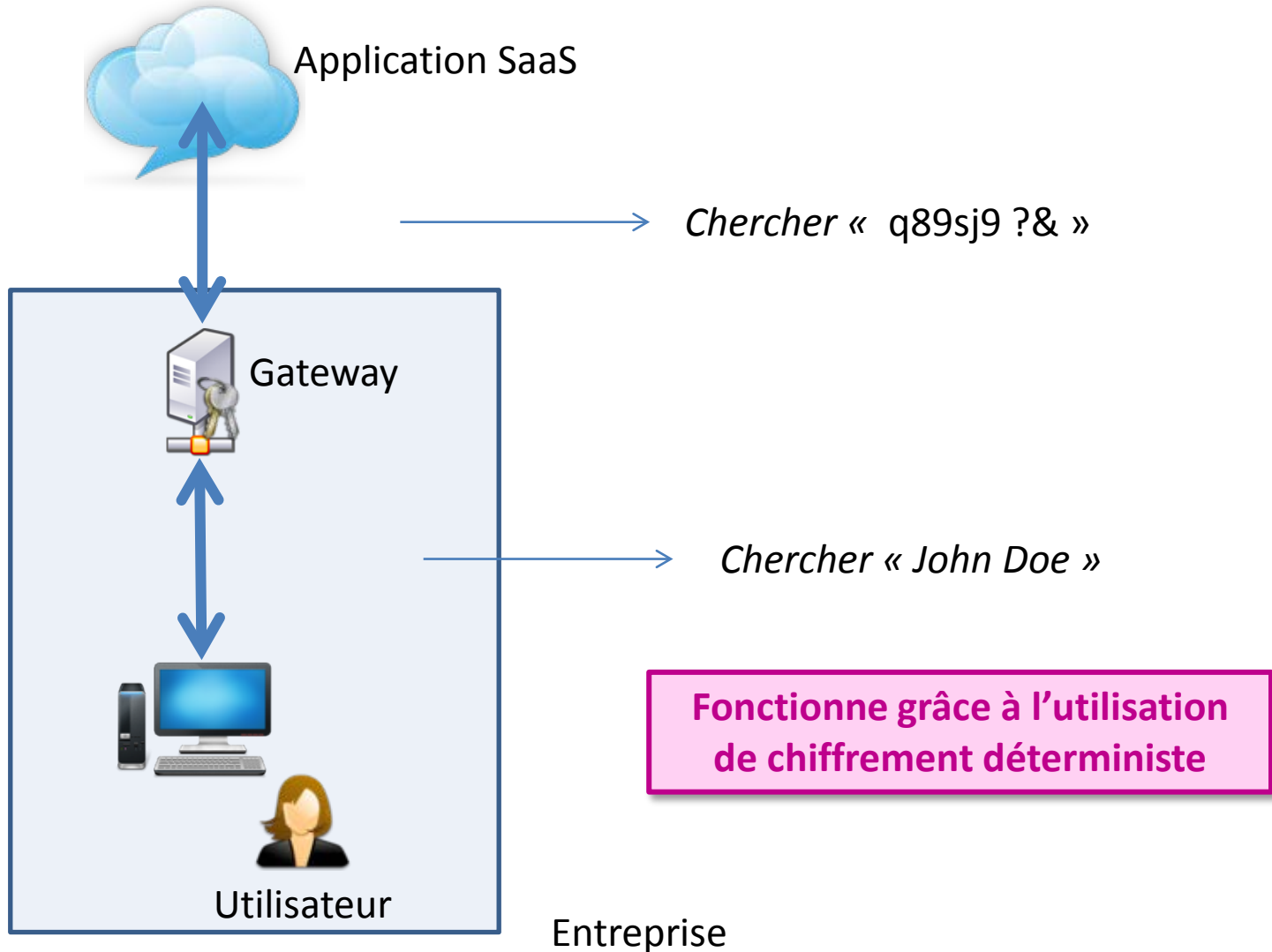
- Peut préserver certaines fonctionnalités :

- Recherche

- Tri




Faire une recherche



Fonctionnement

- L'utilisateur se connecte au gateway

 <https://mail.google-com.gmail.ciphercloud.net/mail/#inbox>

au lieu de l'url de l'application SaaS

 <https://mail.google.com/mail/ca/u/0/?shva=1#inbox>

- Pour le reste : utilisation transparente



CipherCloud

- Cloud Security Gateway
- Applications supportées :



- D'autres en développement
- « Cool Vendor » Gartner (2011)

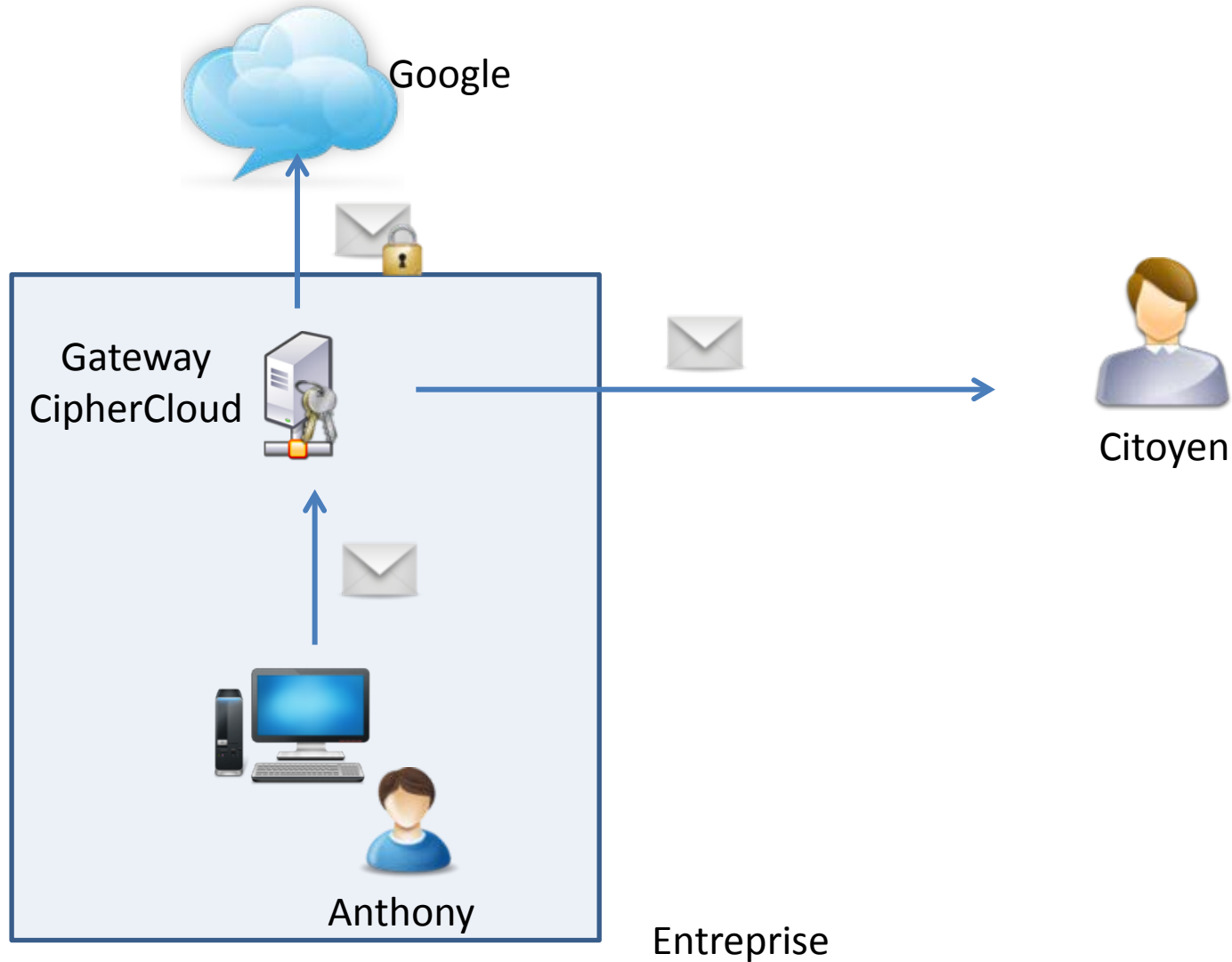


Démo CipherCloud for Gmail

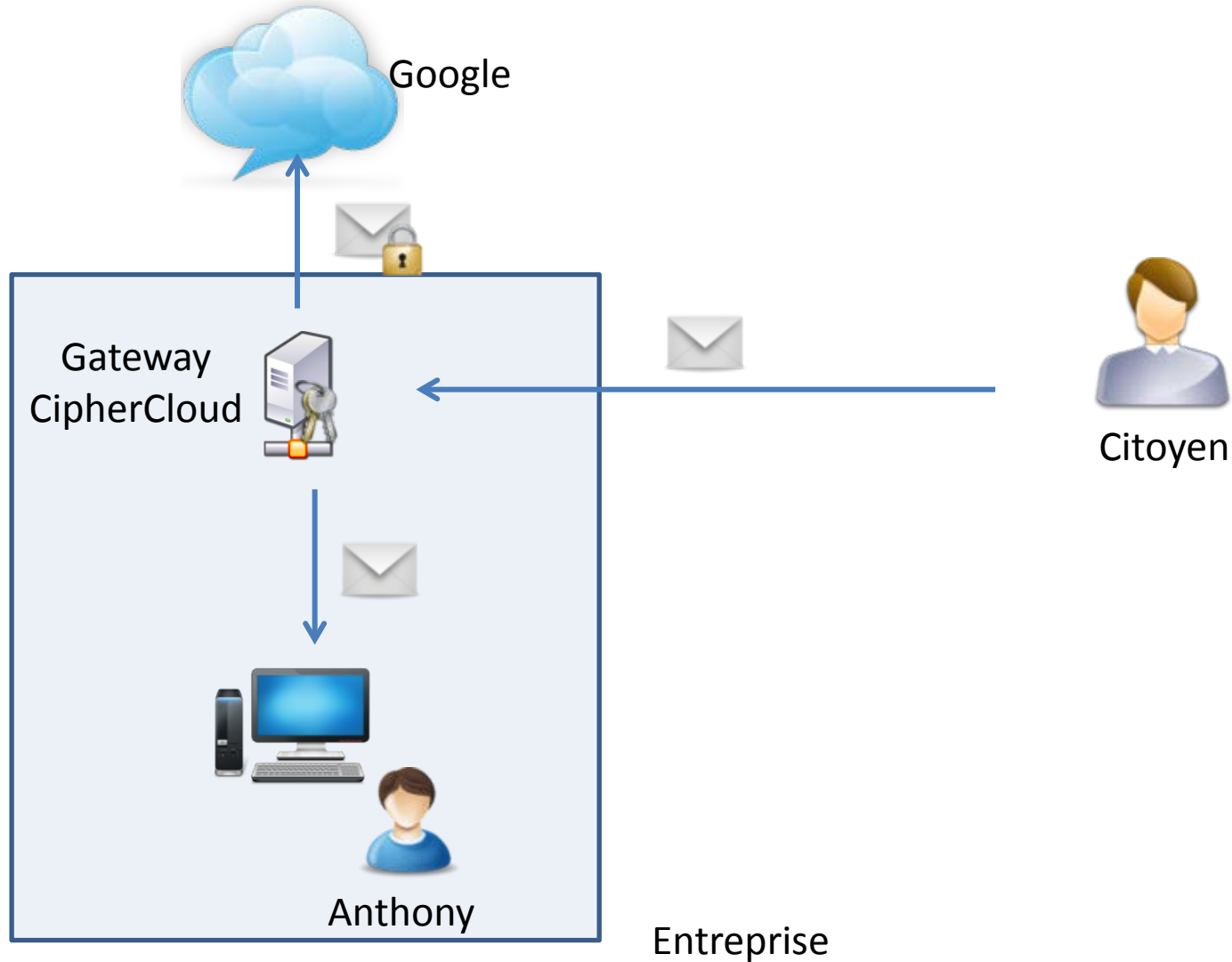
- Scénario :
 - Anthony travaille pour un organisme
 - Il utilise CipherCloud pour Gmail
 - Il échange des emails avec un citoyen
 - Envoi et lecture de mp3
- Configuration de test :
 - CipherCloud installé sur Amazon




Envoi d'un email


















Réception d'un email



Que chiffre CipherCloud ?

 : Chiffré

 : Non chiffré

	Sans CipherCloud	Avec CipherCloud
Expéditeur / Destinataire		
Sujet du mail		
Contenu du mail		
Taille du mail		
Nom des pièces jointes		 / 
Contenu des pièces jointes		
Taille des pièces jointes		



CipherCloud : Opinion

- Avantages :
 - Protège efficacement
 - Contenu des emails
 - Contenu des pièces jointes
- Impact sur les performances :
 - Dépend de la connexion avec le gateway
- Inconvénients :
 - Disponibilité : on devient dépendant de la disponibilité du gateway
 - Tout n'est pas caché aux yeux de Google
 - Chiffrement mot par mot
 - On renonce à certaines fonctionnalités

**Compromis
Sécurité / Fonctionnalité !**



Cloud Security Gateways : marché

- Marché émergeant
- Fournisseurs présents sur le marché:
 - Certes Networks
 - CipherCloud
 - Concealium
 - Intel
 - PerspecSys
 - Symantec

Source : Gartner 2012



Et pour *mon* application ?

- Solution CSG : dépend de la structure de l'application
- Pour une application spécifique (ex : Yammer)
Configurer la CSG avec :
 - les url des applications
 - des *policies*
 - Spécifier des champs à chiffrer ou tokeniser
- Exemple : CipherCloud AnyApp



Conclusion CSG

- Permettent d'utiliser des applications SaaS en protégeant les données
- Marché émergent
- Compromis entre
 - Fonctionnalité
 - Sécurité
- Opportunité : Smals comme Cloud Services Broker



Agenda

1. Introduction
2. Applications de stockage dans le Cloud
3. Autres applications SaaS
4. Smals Threshold Encryption pour le Cloud
5. Recommandations



Cas d'utilisation



- Système de dossiers médicaux
- On veut chiffrer les données
- Sans savoir à l'avance qui sera autorisé à les lire
 - Chiffrement non adressé
- Les solutions de Cloud Encryption ne conviennent pas
 - Pas assez de granularité
 - Chiffrement adressé
- Besoin d'une application spécifique



Smals Threshold Encryption

- Système sécurisé proposé par Smals qui permet

- Écriture

- Lecture

- Stockage



dans une base de données

- Chiffrement non adressé
- Deux « déchiffreurs » externes
- Même si un déchiffreur est compromis, les données sont en sécurité
- Utilise un algorithme de « Threshold Encryption »



Scénario

- Alice est médecin
- Elle veut, avec son PC
 - Consulter le dossier d'un patient
 - Mettre à jour certaines données du dossier
- Ce dossier est stocké dans une base de données sous forme chiffrée



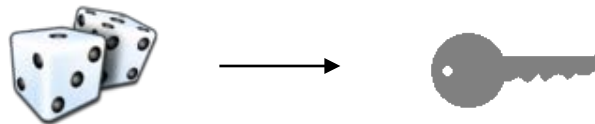
Écriture d'une entrée d'un dossier médical

- Le logiciel d'Alice
 - chiffre l'entrée
 - l'envoie dans la base de données

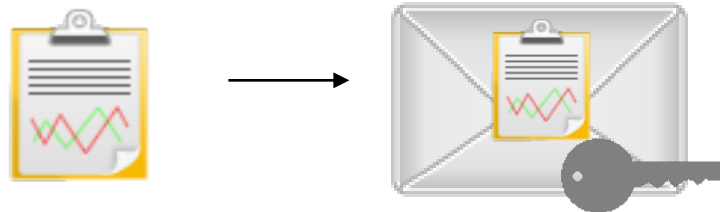


Chiffrement d'une entrée

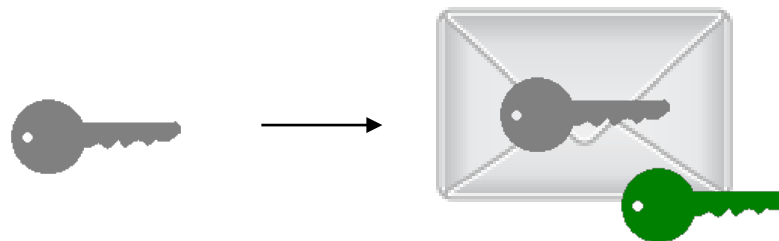
1. Alice génère une clé de session au hasard



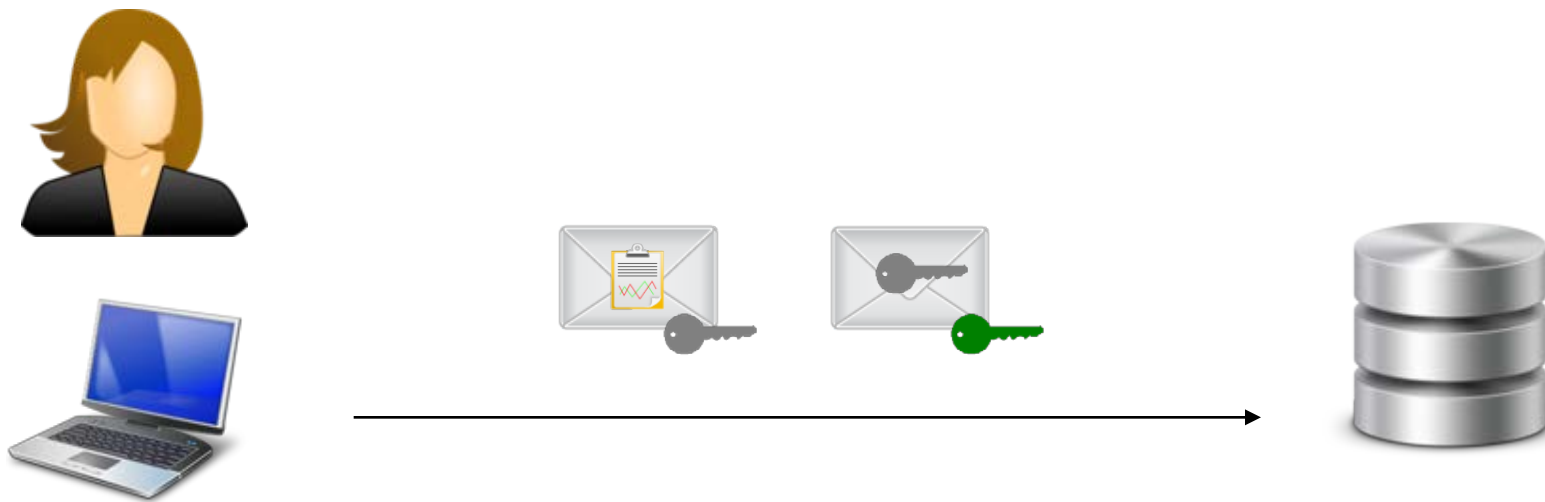
2. Alice chiffre la donnée avec cette clé de session



3. Alice chiffre la clé de session avec la clé publique de la base de données



Envoi dans la base de données



Stockage dans la base de données

- Un champ contient deux valeurs :
 - La donnée chiffrée avec une clé de session



- La clé de session chiffrée avec la clé publique de la base de données



- Clé verte : clé de la base de données, la même pour chaque champ
- Clé grise : différente pour chaque champ



Threshold Encryption

- Si une seule entité avait le pouvoir de déchiffrer la clé de session : risque de sécurité !
- On veut répartir ce pouvoir entre au moins deux entités séparées
- On va donc utiliser un système de chiffrement spécial: "Threshold Encryption" (threshold = seuil, drempe)
- Une clé publique :

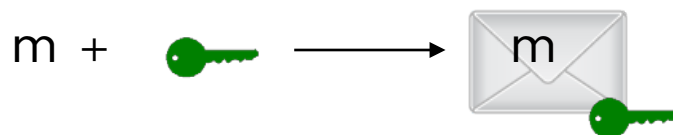


- Deux clés privées :

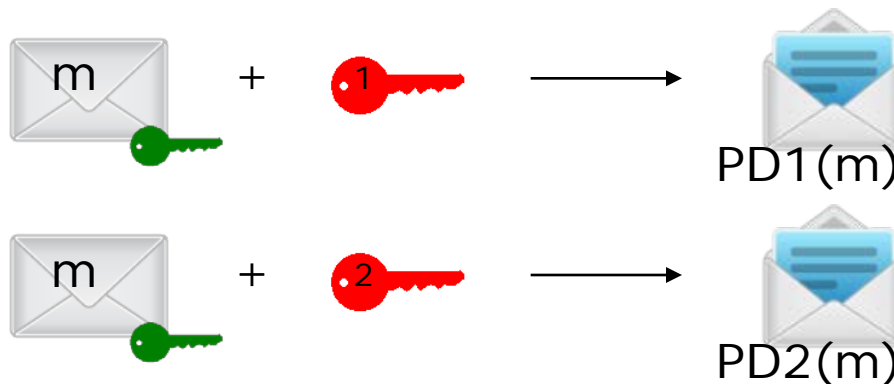


Threshold Encryption

- On chiffre un message avec la clé publique



- Si l'on possède une clé privée on calcule un déchiffrement partiel

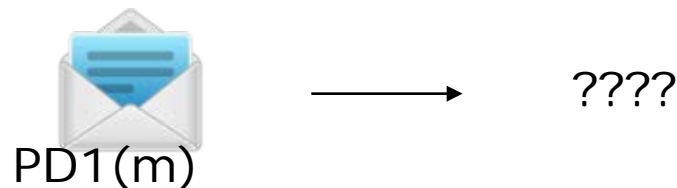


Threshold Encryption

- Celui qui possède les deux déchiffrements partiels peut les combiner pour retrouver le message clair

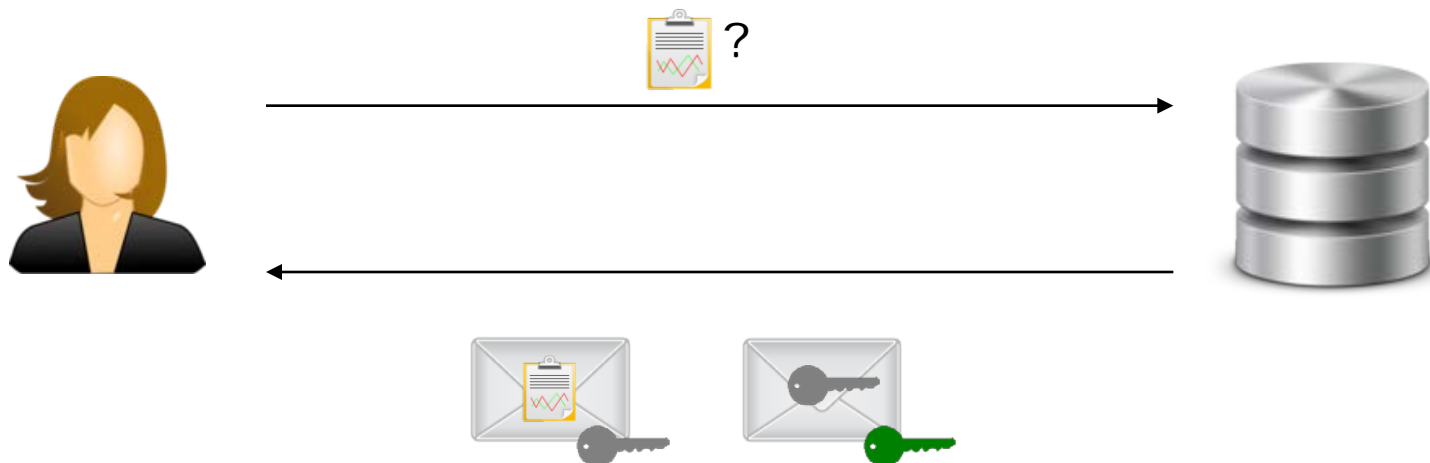


- Avec seulement un déchiffrement partiel, on ne retrouve aucune information sur le message clair



Lecture (phase 1)

1. Alice envoie une requête à la base de données
2. Elle reçoit la donnée chiffrée et la clé de session chiffrée

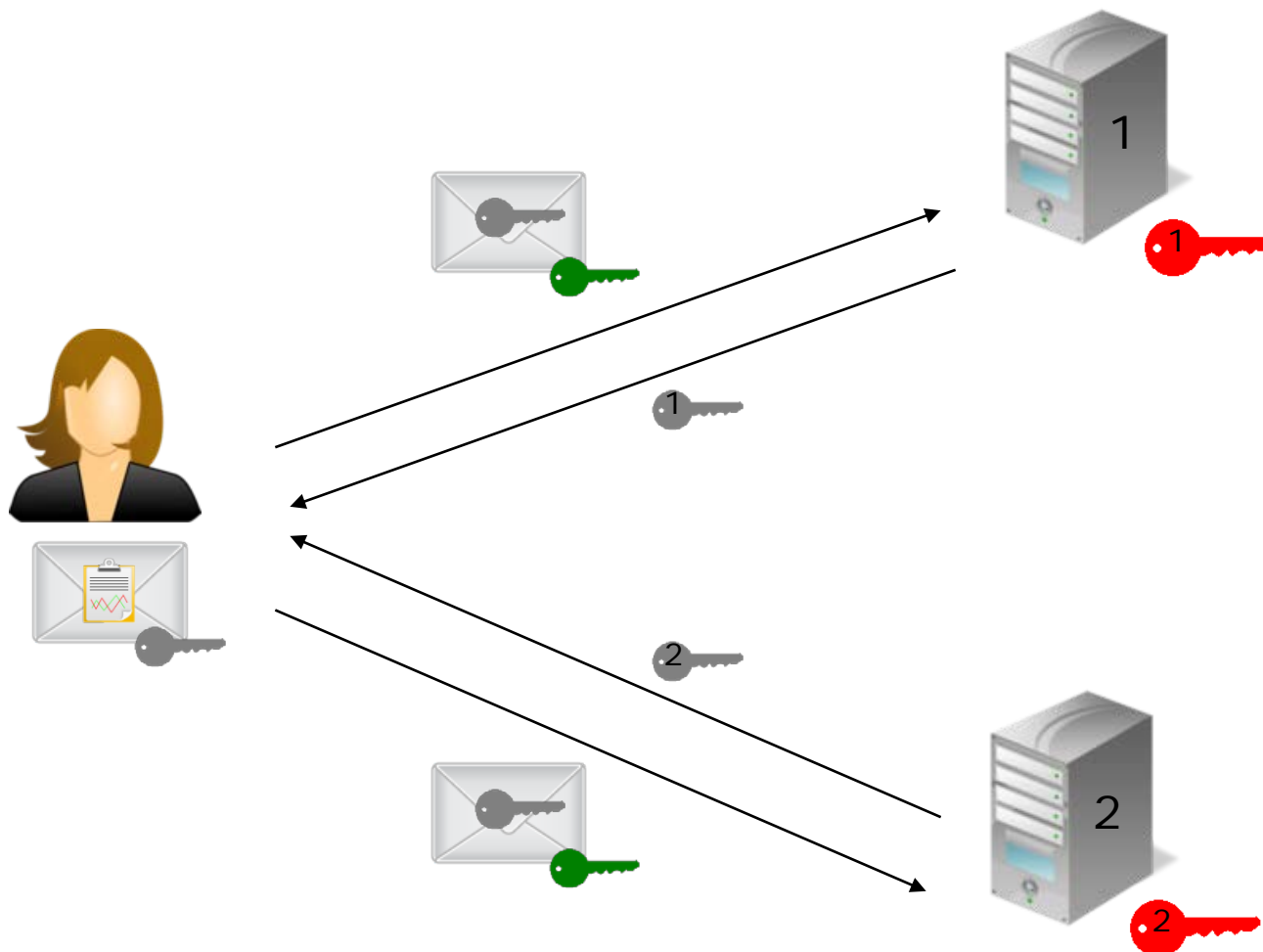


Lecture (phase 2)

1. Alice envoie la clé de session chiffrée à deux "Partial Decryption Servers"
2. Chaque serveur calcule un déchiffrement partiel de la clé de session et l'envoie à Alice (via des tunnels chiffrés)

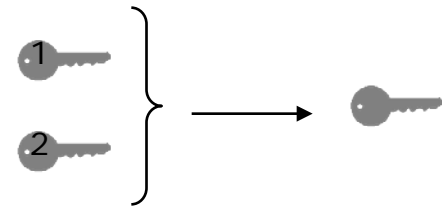


Lecture (phase 2)

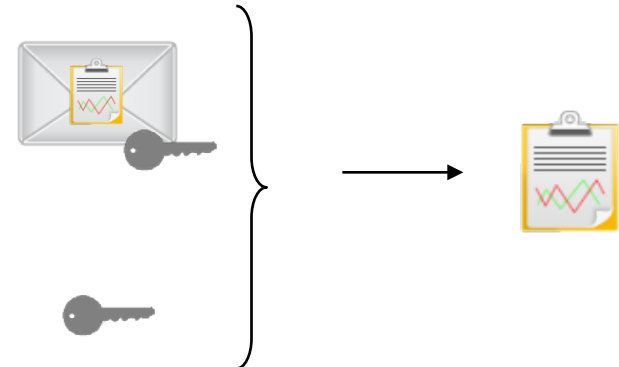


Lecture (phase 3)

1. Alice combine les
déchiffrement partiels pour
reconstituer la clé de session



2. Alice déchiffre la donnée
avec la clé de session




Sécurité du système

- But principal : assurer la confidentialité des données
- Les données sont stockées chiffrées dans la base de données
- Dans le cycle de vie des données, elles apparaissent en clair uniquement sur le PC d'Alice
- Les "Partial Decryption Servers" ne reçoivent jamais les données, même pas sous forme chiffrée (ils ne traitent que des clés de sessions)
- Donc un attaquant passif (qui ne fait qu'espionner les communications) n'obtient aucune information sur les données
- Mais que se passe-t-il si le système est attaqué de l'intérieur ?



Sécurité du système

- Si un administrateur du serveur 1 attaque le système et parvient à :
 - Obtenir la clé 
 - Écouter les communications
 - Accéder au support des données

Sans la clé , il ne peut pas déchiffrer !

- Idem pour serveur 2



Conclusion

- Le système permet
 - D'assurer la confidentialité des données
 - De répartir la confiance entre deux serveurs de déchiffrement partiel (si l'un est compromis, les données restent en sécurité)
 - Que les serveurs de déchiffrement partiel n'aient aucun accès aux données médicales, même chiffrées
- On peut aussi utiliser plus de deux serveurs
 - Plus complexe mais offre une meilleure disponibilité du service



Comparaison

	Threshold Encryption	Cloud Security Gateways
Type d'application	Application spécifique	S'adapte à des applications existantes
Plateforme	Hors de l'entreprise	Dans l'entreprise
Gestion des clés	Décentralisée	Centralisée
Confiance	Distribuée	Centralisée



Quelle solution choisir ?

- Exemple 1 : Dossiers médicaux
 - Chiffrement non adressé
 - Solution adaptée : Smals Threshold Encryption
- Exemple 2 : Gmail
 - Besoin de chiffrer / déchiffrer à la volée les données d'une application
 - Solution adaptée : Cloud Security Gateway



Agenda

1. Introduction
2. Applications de stockage dans le Cloud
3. Autres applications SaaS
4. Smals Threshold Encryption pour le Cloud
5. Recommandations



Recommandations

- Utiliser des solutions de Cloud Encryption adaptées à ses besoins
- Points d'attention :
 - Evaluer le gain réel de sécurité
 - Penser à la disponibilité du service
 - Evaluer les fonctionnalités indispensables



Conclusion

- Stockage Cloud + chiffrement
 - Utilisation relativement transparente
 - Pas d'impact notable sur les performances
 - Vrai gain de sécurité
- Applications SaaS + chiffrement
 - Permet une protection des données
 - On doit renoncer à certains avantages :
 - Fonctionnalités
 - Coût
 - Disponibilité





Questions et remarques bienvenues !



Julien.Cathalo@smals.be

www.smals.be