# CLOUD ENCRYPTION

JULIEN CATHALO



## 1. Introduction

Le cloud computing est une tendance forte dans le monde de l'IT. Ses nombreux avantages, comme la flexibilité d'utilisation ou la réduction des coûts, ont convaincu beaucoup d'entreprises qui utilisent désormais des services et applications cloud comme Dropbox, Gmail ou Salesforce au quotidien.

La sécurité doit faire l'objet d'une attention particulière lors du choix d'une solution de type cloud. En effet, mettre ses données dans le cloud implique a priori que l'on perd le contrôle sur ces données et que l'on fait confiance au fournisseur de services cloud pour protéger ces données. L'un des aspects de cette protection est la confidentialité : que fait mon fournisseur des données confidentielles (les miennes ou celles de mes utilisateurs) ? Même si le fournisseur a pris les mesures suffisantes pour correctement protéger les données par rapport à des attaquants externes, le fournisseur lui-même a accès à ces données et un gouvernement pourrait exiger qu'il les lui transmette (voir l'exemple du Patriot Act aux États-Unis).

Certains produits récents et innovants offrent des solutions de chiffrement pour les organisations qui souhaitent utiliser des services cloud tout en gardant l'assurance de la confidentialité de leurs données. On peut classer ces produits dans deux catégories : d'une part, des solutions de stockage dans le cloud orientés utilisateur avec chiffrement. D'autre part, les « Cloud Security Gateways », conçues pour utiliser des applications cloud spécifiques comme Gmail ou Salesforce. Dans ces deux catégories, un point important est l'approche utilisée pour chiffrer les données : elles sont chiffrées avant d'être envoyées dans le cloud et avec des clés dont l'utilisateur ou l'entreprise garde toujours le contrôle. Ainsi, le fournisseur cloud n'a jamais accès aux clés et ne peut donc pas déchiffrer les données.

# 2. Chiffrement pour stockage cloud orienté utilisateur

## 2.1. Approches possibles

Il existe de très nombreux services de stockage cloud orienté utilisateurs. Quelques un des plus connus sont Dropbox, Google Drive, et Microsoft SkyDrive. Ces services permettent à un utilisateur de stocker ses documents dans le cloud, afin d'y accéder depuis plusieurs appareils, de les partager avec d'autres utilisateurs, ou de disposer d'une forme de backup online.

Dans ce domaine, pour protéger la confidentialité des données par rapport au fournisseur cloud, trois approches sont possibles, et le choix d'une approche doit être fait en prenant en compte la simplicité d'utilisation et le niveau de sécurité voulu.

- Utiliser un service cloud qui offre de bonnes garanties de sécurité et permet le chiffrement des données localement.

Dans cette catégorie, nous recommandations SpiderOak, qui offre un produit complet et dont la sécurité est particulièrement bien pensée. Cependant, l'application mobile (version testée : Android) manque de fonctionnalités : il n'est pas possible de partager des données stockées sur le mobile.

- Utiliser un outil dédié qui chiffre les données localement en combinaison avec un service cloud qui synchronise les données.

Dans cette catégorie, nous avons testé BoxCryptor qui est simple d'utilisation mais limite les fonctionnalités de partage. Cloudfogger, dans sa version actuelle au moment où sont tapées ces lignes (1.2.1875 Windows, 1.0.1936 Mac OS), permet de partager les données ; il est donc plus intéressant.

- Utiliser un outil de chiffrement plus généraliste comme Truecrypt et synchroniser le container avec le service cloud.

Cette solution offre un excellent niveau de sécurité, mais présente deux inconvénients : elle est plus complexe d'utilisation, et elle limite les possibilités de partage.

## 2.2. Recommandations

Aucune solution actuelle n'est complètement satisfaisante.

Si le partage de documents n'est pas nécessaire, nous recommandons :

- CloudFogger, à utiliser en combinaison avec SkyDrive, Dropbox ou Google Drive
- SpiderOak

- TrueCrypt, à utiliser en combinaison avec SkyDrive, Dropbox ou Google Drive

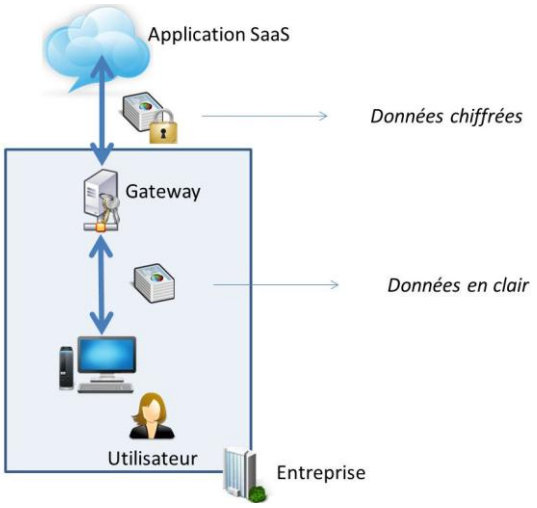
Dans tous les cas, c'est l'utilisation via mobile qui est limitée : les applications mobiles permettent seulement de lire les données depuis le mobile mais pas de synchroniser un répertoire présent sur le mobile.

Si le partage de documents est nécessaire, TrueCrypt va être trop contraignant. La recommandation dans ce cas devient donc :

- CloudFogger, à utiliser en combinaison avec SkyDrive, Dropbox ou Google Drive
- SpiderOak

## 3. Chiffrement pour autres applications SaaS

Les Cloud Security Gateways sont des produits conçus pour permettre aux employés d'une organisation d'utiliser des applications SaaS tout en chiffrant tout ou partie des données de l'application. Le principe est d'utiliser un gateway qui est localisé soit dans l'organisation soit chez un tiers. Voici un schéma qui démontre le cas où le gateway est dans l'organisation :




Ce marché est émergeant et de nombreuses solutions sont en train d'apparaître. Les principaux acteurs sont Certes Networks, CipherCloud, Concealium, Intel, PerspecSys, Symantec. Chaque produit vise une application SaaS spécifique ; parmi les plus souvent rencontrées, on peut citer Salesforce, Office 365 ou Gmail.

Dans la suite nous nous concentrons sur CipherCloud for Gmail.

Dans le cadre de cette étude nous avons procédé à un Proof of Concept de CipherCloud for Gmail. Ce produit permet d'utiliser Gmail au sein d'une organisation tout en empêchant Google de pouvoir lire le contenu des mails et des pièces jointes. Les conclusions du POC sont que le produit permet que le contenu des messages et des pièces jointes soit efficacement protégé mais présente les inconvénients suivants :

- Impact sur les performances : l'utilisation entraîne une latence qui dépend notamment de la connexion avec le gateway.
- Impact sur la disponibilité : on devient dépendant de la disponibilité du gateway, en plus de celle du fournisseur SaaS.
- Impact sur les fonctionnalités : certaines (comme la recherche dans les mails) sont préservées, mais d'autres (comme les lecteurs intégrés à Gmail pour lire des mp3 ou d'autres types de fichiers) ne marchent plus.
- Coût du gateway (licence) qui vient s'ajouter au coût de l'application elle-même et nécessité d'administrer le gateway.
- Limites en termes de sécurité : tout n'est pas caché aux yeux de Google. Ainsi, les expéditeurs, destinataires, la taille des messages sont accessibles en clair par Google.

En conclusion, le choix d'un produit comme CipherCloud permet une meilleure sécurité (protection contre le fournisseur SaaS, dans ce cas Google), mais demande de renoncer à certains des avantages du SaaS.

Comme déjà mentionné, le gateway peut aussi être hébergé chez un tiers. Smals pourrait assumer cet hébergement pour nos membres et prendre ainsi le rôle de Cloud Services Broker ; cela permettrait une réduction du coût et de la gestion pour le client.