CNIL.

Note interne

Date : 21/08/2018

Émetteur	Destinataires	Pour information
[redacted]	[redacted]	

Objet : Le chiffrement dans Office 365

Cette note a pour objet de recenser les mécanismes de chiffrement mis en œuvre au sein d'Office 365. Une présentation des différentes fonctionnalités mises en place, par défaut ou en option, est réalisée afin de rendre compte des garanties apportées et des points de vigilance identifiés.

Depuis 2011, Microsoft propose une version de sa suite « Microsoft Office » sous forme d'abonnement mensuel ou annuel, à destination des particuliers et des entreprises de toutes tailles. Dénommée « Office 365 », cette suite est liée à un compte utilisateur Microsoft et non plus à un terminal unique avec une installation pérenne. Via internet, il est possible de synchroniser ses documents qui sont enregistrés dans le Cloud et donc accessibles depuis plusieurs terminaux. Nous dressons ici un panorama des différents outils de chiffrement associés, disponibles par défaut ou non. Étant donné que ce document est construit à partir de ressources publiquement accessibles sur le site internet de Microsoft, il est important de préciser qu'il n'est pas nécessairement exhaustif. En effet, l'offre de services Office 365 se décline à travers plusieurs suites[1] destinées aux entreprises de toutes tailles. En fonction des services utilisés, elles font appel à des outils de sécurité différents, parfois complémentaires, qui peuvent également être liés aux architectures utilisées dépendantes ou non de Microsoft.

1 Par défaut

1.1 Chiffrement des données

Dans son offre de base, Office 365 met en œuvre du chiffrement à la fois pour les données échangées et pour celles stockées en base.

Pour les flux de données, le protocole TLS est utilisé pour l'ensemble des échanges, à savoir :

- tout échange entre un terminal client et les serveurs Office 365 ;
- tout échange entre les serveurs Office 365 et un serveur externe ;
- tout échange au sein des datacenters Office 365, qui peut également être réalisé via IPSEC.

À noter qu'à compter du 31 octobre 2018, Office 365 ne fonctionnera qu'avec TLS 1.2 et ne supportera plus les versions antérieures (1.0 et 1.1) ; il en est de même pour le 3DES. En outre, l'ensemble des suites cryptographiques supportées sont visibles en ligne[2].

Pour les données au repos, Microsoft sécurise ses serveurs Office 365 avec BitLocker, détaillé ci-après, qui permet de chiffrer les disques contenant des données clients. Des mécanismes de chiffrement sont également mis en œuvre au niveau des fichiers avec des gestions distinctes selon le type de données échangées (ex : mails vs fichiers). Sur le terminal de l'utilisateur, en local, BitLocker peut également être utilisé.

[1] L'annexe 1 présente succinctement les différentes suites Office 365 proposées aux entreprises par Microsoft.
[2] Les suites cryptographiques possibles sont les suivants :
- échanges de clés via ECDHE ou RSA ;
- authentification via RSA-2048 minium ;
- chiffrement AES-128 minimum ou 3DES-192 jusqu'en oct. 2018;
- mode de chiffrement CBC ;
- empreinte SHA-256 minimum.

BitLocker est une solution de chiffrement apparue avec Windows Vista pour assurer la confidentialité des données et plus particulièrement le chiffrement de volume du système d'exploitation ou volume de données. Pour Office 365, BitLocker chiffre les disques contenant des données clients (Exchange Online, SharePoint Online, Skype for Business) avec l'algorithme AES-256 bits. BitLocker fonctionne de façon standard avec :

- une clé FVEK (*Full Volume Encryption Key*), utilisée pour chiffrer le disque ; elle doit être bien protégée puisqu'impossible à changer sans déchiffrer/rechiffrer le volume ;
- une clé VMK (*Volume Master Key*), pour chiffrer et protéger la clé précédente ; elle peut être modifiée en cas de compromission sans devoir changer la FVEK ;
- le module TPM (*Trusted Platform Module*), pour protéger la clé VMK.

Dans la version standard, par défaut, les clés utilisées sont stockées et gérées directement par Microsoft. Sans aucune configuration ni connaissance en cryptographie, ce chiffrement est totalement transparent pour le client. Il n'a aucun contrôle ou accès aux clés de chiffrement et n'est pas en capacité de le désactiver.

1.2 Spécificités et options

Selon l'offre souscrite ou le service utilisé, des mécanismes supplémentaires sont mis en œuvre.

Azure Storage Service Encryption est le service de chiffrement mis en œuvre dans l'offre d'hébergement et de services cloud Microsoft Azure pour les entreprises. Les données sont automatiquement chiffrées pour y être stockées. Les modalités de gestion de clé semblent identiques à celles possibles avec Microsoft Office 365 détaillées par la suite. Pour certains services Office 365, ce service de chiffrement est utilisé.

Azure Information Protection (AIP) est la solution cloud qui permet de contrôler un document même si celui-ci est partagé avec d'autres personnes, en interne comme hors de l'entreprise. Ainsi, AIP peut être utilisé pour classifier et/ou protéger des documents et des mails, de façon automatique selon les règles administrateurs ou bien manuellement (ex Microsoft : un numéro de carte bancaire est inscrit dans un document, celui-ci est étiqueté comme sensible, par exemple, et éventuellement protégé). Un tel document peut faire l'objet d'un suivi et d'un contrôle pour détecter des comportements à risque, appliquer les mesures jugées adéquates, empêcher une fuite de données, *etc.* En particulier, dans le cadre d'Office 365, AIP offre la possibilité de gérer des droits d'accès à l'information via IRM (*Information Right Management*), fournie par défaut dans les versions Entreprise E3 ou E5 ou en option sinon. Comme nous le verrons par la suite, l'accès à AIP joue un rôle non négligeable dans les outils de chiffrement disponibles.

Office 365 Message Encryption (OME) permet de chiffrer simplement des messages envoyés et de gérer les droits d'accès. Ce service repose sur AIP et est donc inclus dans les offres Entreprises E3 et E5. L'apport de OME est de se prémunir des risques d'attaques *man-in-the-middle* ou encore d'éviter un accès illégitime aux données par un utilisateur n'ayant pas les droits, au sein de l'entreprise comme à l'extérieur. Des politiques automatiques peuvent être définies par les administrateurs. L'utilisateur peut appliquer de lui-même ces protections à travers son outil Outlook, version en ligne ou logiciel.

Exchange Online. Pour les boîtes Exchange Online, BitLocker est également utilisé. Les utilisateurs utilisant « Customer Key » (décrit par la suite) peuvent ajouter une couche supplémentaire. Ainsi, ce n'est pas uniquement le volume de stockage qui est chiffré mais bien les données de la boîte Exchange Online. Une version par défaut, gérée par Microsoft, serait prévue. À noter que ces mesures s'appliquent également à Skype for Business qui stocke la plupart du contenu utilisateur au sein des boîtes Exchange.

Skype for Business. Les documents/présentations partagés lors d'une conférence par Skype peuvent être stockés comme fichiers. Le serveur dédié chiffre ces données avec l'algorithme AES-256 bits. Elles sont stockées dans un fichier partagé où chaque information est chiffrée avec une clé différente et aléatoire. Plus formellement, quand un élément est partagé sur une conférence, le serveur demande aux clients de télécharger par HTTPS les données chiffrées. La clé requise est envoyée aux clients qui peuvent alors déchiffrer. Le serveur authentifie les clients avant de leur permettre l'accès (protocole SIP via TLS puis cookies d'authentification).

SharePoint Online. Tout fichier stocké dans SharePoint Online est également chiffré en AES-256 bits avec une clé par fichier et ce pour chaque client. Dans la version standard, ces clés sont par défaut gérées et créées par le service. SharePoint Online chiffre les fichiers avant de les envoyer dans l'hébergement Azure qui n'a pas la possibilité de déchiffrer ou d'obtenir de l'information sur les données. Plusieurs services Office 365 stockent leurs données dans SharePoint (ex : Microsoft Teams[3] et **OneDrive for Business**).

[3] Microsoft Teams est une application permettant de créer, partager et collaborer facilement en équipe à partir de tout terminal (plateforme commune personnalisable, discussions en groupe, notes, réunions visio, etc.), avec accès à SharePoint, OneNote et Skype.

2 Possibilités de gestions des clés cryptographiques

2.1 (Presque) sous le contrôle du client

Microsoft laisse la possibilité au client de gérer lui-même les clés en mettant en avant deux cas d'usage :

1. le respect de la règlementation[4] propre aux pays du client qui imposerait des besoins de sécurité (lieu de stockage des clés, gestion et accès) ;
2. l'utilisation de HSM par certaines organisations qui souhaiteraient utiliser ces mêmes clés pour le cloud.

Seuls certains services semblent concernés par cette possibilité (Exchange Online, Skype for Business, SharePoint Online et OneDrive for Business). Comme pour le cas par défaut, une distinction est faite entre les données au repos et les flux.

Azure Key Vault (AKV) est l'outil qui permet de protéger et de gérer les secrets utilisés par les services/applications cloud dans un module de sécurité matériel (HSM), conforme au FIPS-140. Les clés, secrets et éventuellement mots de passe peuvent être chiffrés à partir de clés stockées dans des HSM. C'est la solution recommandée par Microsoft pour la gestion et le contrôle des clés. Une séparation des rôles existe alors entre les administrateurs en charge de la sécurité des données et ceux ayant en charge la gestion des clés. Microsoft n'accède pas aux clés stockées via AKV, tout comme les applications n'ont pas d'accès direct. Tout accès peut être journalisé.

***Customer Key* avec AKV.** À travers l'utilisation de AKV, le client peut importer et contrôler ses propres clés de chiffrement pour les données **au repos**. La clé racine ne quitte jamais le HSM, le client contrôle ses clés et peut les révoquer s'il décide de quitter le service (entraînant la perte de l'accès aux données associées).

Cependant, Customer Key intègre une clé dite de disponibilité, pour parer au risque de perte des données. C'est en réalité une **clé maître, fournie et protégée par Microsoft** qui fonctionne comme les clés fournies par le client. L'existence de cette clé est justifiée par la difficulté que représentent la gestion et la protection des clés pour le client ainsi que la nécessité pour Microsoft d'assurer la qualité de service. Ne pas pouvoir atteindre les clés du client dans AKV (ex : problème réseau) rendrait les services d'Office 365 inopérants d'où le recours à la clé de disponibilité si besoin. Cette clé est unique pour chaque client et supprimée s'il décide de quitter le service.

Bring Your Own Key (BYOK) avec AIP. De même, pour les **flux de données**, le client a la possibilité de fournir ses propres clés. L'exemple donné par Microsoft est OME où il est possible de choisir les clés pour les messages sensibles. Dans ce cas, la sécurité de la messagerie repose sur AIP qui prend en charge la gestion des clés et l'interfaçage avec AKV qui réalise le chiffrement ; les clés restent protégées dans le HSM. La clé racine utilisée peut soit être générée directement dans AKV soit créée sur site et transférée/importée ensuite dans AKV.

2.2 Maîtrise totale du client sur site ou hybride

Enfin, Microsoft considère également le cas où des organismes doivent avec un contrôle total sur les clés utilisées. Néanmoins, cette option est présentée comme étant destinée à un « très petit sous-ensemble d'organismes hautement règlementé » et pour des « données vraiment très sensibles ».

Hold Your Own Key (HYOK) avec AIP. HYOK est pris en charge par AIP quand Azure Directory Rights Management Service (AD RMS) est déployé « On premise ». Ainsi, le client peut utiliser des clés stockées et gérées sur site. Les données sont alors accessibles uniquement aux applications et services en local. Les données seront inintelligibles à toutes personnes extérieures, Microsoft inclus.

Selon Microsoft, HYOK n'est pas destiné à tous les acteurs et ne devrait pas concerner toutes les données. HYOK est plutôt présenté comme un simple outil qui répond à un besoin précis à savoir l'opacité à tout prix. Microsoft recommande de n'utiliser cette solution que pour moins de 1% des données. Les données n'étant plus accessibles à Microsoft, certains services s'en trouvent dès lors diminués : protections anti malware, anti spam, Delve (agrégateur d'informations), eDiscovery (gestion de la conformité), outils de recherche, etc. De même, les règles de transports ou politiques de DLP ne sont plus capables de consulter les données.

S/MIME. En outre, il est également possible d'utiliser S/MIME, standard pour sécuriser les échanges par courriers électroniques (chiffrement et signature). Les certificats utilisés sont fournis via l'AD et les clés privées

[4] Un des exemples donnés par Microsoft est le secteur financier (lutte anti-fraude, anti-blanchiment, etc.) avec les réglementations/normes SEPA, MiFID ou encore PCI-DSS.

elles restent sur site et ne sont jamais transmises à Office 365. Par conséquent, comme précédemment, les services qui nécessitent l'accès à ces données ne fonctionneront pas.

3 Conclusion

À travers cette analyse, nous avons pu constater que Microsoft intègre, par défaut, des algorithmes de **chiffrement à l'état de l'art** (ex : AES 256), conforme à l'annexe B1 du référentiel de sécurité. Les **flux** de données sont chiffrés et les **supports** également, évitant ainsi les risques d'accès illégitime aux données et de l'interruption de flux.

Il n'est cependant pas évident de se repérer dans les spécificités additionnelles propres à chaque service et les propriétés supplémentaires qui sont parfois apportées. Il est important de bien préciser que les services mentionnés ne sont pas tous disponibles pour n'importe quel client mais que cela dépend des offres souscrites. En particulier, il semble que ce soit surtout les offres Entreprise E3 et E5 qui permettent le plus de latitude en matière de sécurité mais elles sont également les plus chères. De plus, de nombreux autres services (outre Skype, OneDrive, Exchange, SharePoint) sont fournis avec Office 365. Nous supposons que leur sécurité dépend propriétés de sécurité héritées des services principaux.

La **gestion des clés** et des secrets est un élément central qui peut être opérée selon différents modes :

1- par défaut, Microsoft génère et gère l'ensemble des clés, sans que le client puisse avoir une quelconque maîtrise, ni conscience du chiffrement mis en œuvre ;
2- une première marge de manœuvre est l'activation d'une clé client pour les données au repos et du recours à BYOK pour les flux de données mais s'accompagne néanmoins de l'existence d'une clé maître détenue par Microsoft ;
3- enfin, le client peut utiliser ses propres clés, qui restent entièrement sous son contrôle sans que Microsoft puisse accéder aux données concernées mais cela implique par conséquent l'inefficacité de certains services cloud.

Dans sa documentation publique, Microsoft insiste sur le fait qu'utiliser du chiffrement avec pour but de rendre inintelligible les données au service de cloud a pour conséquence de bloquer les propriétés innovantes fournies par les services déployés qui sont justement la raison d'y souscrire.

Annexes

Annexe 1 – Offres Microsoft Office 365 pour les entreprises

Microsoft décline trois offres pour les petites et moyennes entreprises, pour 300 utilisateurs maximum.

		Business	Business Premium	Business Essentials
Logiciels	Outlook	Inclus	Inclus	Non inclus
	Word			
	Excel			
	PowerPoint			
	OneNote			
	Access			
	Publisher			
Web	Word	Inclus	Inclus	Inclus
	Excel			
	PowerPoint			
Services[5] « collaboratifs »	Exchange	**Non inclus**	Boîtes de 50 Go, adresse avec nom de domaine personnalisé	Boîtes de 50 Go, adresse avec nom de domaine personnalisé
	OneDrive	1 To de stockage	1 To de stockage	1 To de stockage
	SharePoint	**Non inclus**	Inclus Skype en visio : 250 participants max	Inclus Skype en visio : 250 participants max
	Teams			
	Yammer			
	Planificateur			
	Skype Entreprise			
	Bookings			Non inclus
	StaffHub			Non inclus

Au-delà de 300 utilisateurs, des offres dédiées sans nombre maximal d'utilisateurs sont proposées.

		ProPlus	Entreprise E1	Entreprise E3	Entreprise E5
Logiciels	Outlook	Inclus	**Non inclus**	Inclus	Non inclus
	Word				
	Excel				
	PowerPoint				
	OneNote				
	Access				
	Publisher				
Web	Word	Inclus	Inclus	Inclus	Inclus
	Excel				
	PowerPoint				
Services[5] « collaboratifs »	Exchange	**Non inclus**	Boîtes de 50 Go, adresse avec nom de domaine personnalisé	Boîtes de 100 Go, adresse avec nom de domaine personnalisé	Boîtes de 100 Go, adresse avec nom de domaine personnalisé
	OneDrive	1 To de stockage	1 To de stockage	*illimité*	*illimité*
	SharePoint	**Non inclus**	Inclus Skype en visio : 250 participants max	Inclus Skype en visio : 250 participants max	Inclus Skype en visio : 250 participants max
	Teams				
	Yammer				
	Planificateur				
	Skype Entreprise				
	Bookings				Non inclus
	StaffHub				Non inclus

Extrait du site de Microsoft : « Avec Office 365 vos données sont sécurisées et hébergées en France conformément au cadre réglementaire Français et Européen (RGPD). »

Annexe 2 – Références

Les deux principaux documents de références pour le chiffrement mis en œuvre dans Office 365 sont :

- *Introduction to Encryption in Office 365, version actuelle au 13/02/2018 ;*
- *Encryption on the Microsoft Cloud, version actuelle au 02/01/2018.*

Les sites support et blog de Microsoft sont tous deux des mines d'informations pour comprendre plus en profondeur les fonctionnements et disponibilités des services.

[5] Liste non exhaustive.